

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 674 290 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
07.01.2004 Bulletin 2004/02

(51) Int Cl.⁷: **G07F 7/10**, G06K 19/073

(21) Application number: **94402624.4**

(22) Date of filing: **18.11.1994**

(54) Card type storage medium and card type storage medium issuing apparatus

Kartenartiges Speichermedium und Ausgabeapparat für kartenartiges Speichermedium

Support de mémoire du type carte et appareil pour délivrer ce type de support

(84) Designated Contracting States:
DE FR GB

(30) Priority: **25.02.1994 JP 2821294**

(43) Date of publication of application:
27.09.1995 Bulletin 1995/39

(73) Proprietor: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211 (JP)

(72) Inventor: **Hoshino, Masao, c/o Fujitsu Limited**
Kawasaki-shi, Kanagawa 211 (JP)

(74) Representative: **Joly, Jean-Jacques et al**
Cabinet Beau de Loménie
158, rue de l'Université
75340 Paris Cédex 07 (FR)

(56) References cited:

EP-A- 0 292 658	EP-A- 0 563 997
EP-A- 0 583 006	WO-A-94/24673
WO-A-95/01618	US-A- 4 801 787
US-A- 4 877 945	US-A- 4 922 456
US-A- 4 988 855	US-A- 5 091 939

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 674 290 B1

Description

BACKGROUND OF THE INVENTION

(1) Field of the Invention

[0001] The present invention relates to a card type storage medium such as an IC card used as a cashless card, an identification (I.D.) card, a health management card, a municipal corporation card, etc. and an issuing apparatus issuing such card type storage medium.

(2) Description of the Related Art

[0002] A card type storage medium, for example, an IC card having an integrated circuit therein has been widely spread in recent years.

[0003] A file controlling program is set into the IC card to retain data therein so that the data to be processed by an external application program that is incorporated within a terminal apparatus, a host computer or the like can be managed in each file as a unit.

[0004] Referring to FIG. 17, a typical IC card 100 comprises a terminal (a contact or a data communication mechanism) 110, a storage 120 and a control unit 130.

[0005] When the IC card 100 is inserted into an IC card reader/writer (not shown) of a terminal apparatus, a host computer or the like, the terminal 110 is brought into contact with a terminal of the IC card reader/writer to send and receive a signal.

[0006] The storage 120 has a file area in which data to be processed by each various application program is retained in each file, and a directory area 123 which retains control information about each data file 122 held in the file area 121.

[0007] The control unit (MPU: micro processor unit) 130 is to manage the data retained in the file area 121 in the storage unit 120 on the basis of the control information stored in the directory area 123 in the storage unit 120.

[0008] Some IC card has an electric source therein, and some IC card needs to be supplied an electric energy from a terminal apparatus or a host computer by being inserted into the terminal apparatus or the host computer. In the latter case, a nonvolatile storage such as an EEPROM is used as the storage unit 120.

[0009] Such IC card 100 is used as a cashless card, an ID card, a health management card, a municipal corporation card, etc.

[0010] In department stores, super markets, etc., a POS system has been accomplished with employment of a cashless card such as a prepaid card or a credit card for sales promotion. If the IC card is used as such cashless card, it is essential to provide a function for advance payment or future payment to the cashless card, for example, the prepaid card or the credit card.

[0011] If the IC card 100 is used as an ID card to improve convenience in, for example, an intelligent build-

ing, the IC card needs to have a function to hold data about entrance and retrieval to and from the room, attendance of employees, etc. in the data files 122.

[0012] If the IC card 100 is used as a health management card in a hospital, a fitness facility or the like to improve convenience, the IC card 100 has to hold various data such as appointment, carte, results of examination and measurement for the management.

[0013] Likewise, if the IC card 100 is used as a municipal corporation card to improve use of public facilities or administrative service, the IC card holds data about appointment of the facilities, automatic issue of various applications as data files 122 therein.

[0014] The IC card 100 shown in FIG. 17 has predetermined personal identification number (hereinafter, referred as PIN) for every data file 122 retained in the storage unit 120 in order to reinforce the security of the data retained in the IC card 100. Each of the PIN is held as control information in the directory area 123 in the storage unit 120.

[0015] In order to gain an access from an external application or the like, only when a PIN sent with the access is in coincidence with the PIN retained in the directory area 123 in the storage unit 120, the control unit 130 allows reading or updating of the data retained in the data file 122.

[0016] The PIN for each data file 122 is set when the IC card 100 is issued by a card issuing apparatus (not shown). Management of the PIN set by the card issuing apparatus, which varies from each other depending on a card owner, is carried out by another host computer (not shown) different from the card issuing apparatus.

[0017] If a person owning the IC card accidentally forgets a PIN of his or her own IC card 100, the PIN is read out from the host computer managing the PIN through a terminal apparatus which can gain an access to the host computer to verify the PIN.

[0018] The host computer manages the PINS of the owners of all issued IC cards (card type storage media) 100. In addition, it is sometimes necessary to set plural different PINs to every data files in each IC card. The host computer therefore requires a large area in the storage to manage the PINs. The management of the PINs is, therefore, quite complex and troublesome to the entire IC card system. Moreover, in the event of an accident, use of a terminal apparatus accessible to the host computer is indispensable to verify the IC card. Such verification of the IC card causes inconvenience to users of the IC card.

[0019] Meanwhile, a card type storage medium, which is used ahead of an IC card, for example, a magnetic card, is operated in a mode where the stored data is unchangeable as personal identification information (ID). An IC card 100 as above is used in a mode where stored data (for example, information about an amount of money) is variable, as represented by a cashless card.

[0020] In such mode of use, the IC card is used as a

cashless card. In the event of an accident such as system down, power-source break-down, pull-out of the IC card 100 in the course of an updating process to receive money or for account settlement, a failure may develop in data in the data file 122 in the IC card 100. At present, it is impossible to repair or restore (data recovery) such failure in data within the IC card 100.

[0021] To cope with such event, a presently conducted technique is to set an area of 1 byte referred as BCC (block check character) in each record of data held in the data file 122 of the IC card 100, adjust the BCC such that a bit number in each record becomes an even number or an odd number and write the BCC in each record to make a check on the bit number in each record as to whether the bit number is an even number or an odd number upon reading out the data. For instance, in the case where the BCC is so adjusted that the bit number in each record is an even number, if the bit number in the record is an odd number upon checking, some action is taken upon check-out such as to prohibit the IC card 100 from being used.

[0022] It is, however, impossible to detect a system failure as conflicting data developed between the records by such BCC check, as shown in FIG. 18.

[0023] Namely, in the case where data writing and updating are executed a plurality of times (three times in FIG. 18) as one unit of process in the course from an open to close of the IC card 100 by the application program 200 of an external terminal apparatus or the like, if a system failure occurred before the second updating after the first record was updated, it is impossible to detect the system failure by the BCC since no conflict occurred in data as a record unit held in the IC card 100.

[0024] Since the BCC checks a number of bits by a record unit, if 2 bits (an even bit) are left out, or the number of bits are the same but their represented value are different (for example, "0111" and "1011", if three bits), it is impossible to detect such failure as conflicting data.

[0025] In consequence, for example, as shown in FIG. 19, if a system failure occurred while one record is being written into the IC card 100, causing a situation that there exist an updated part and an unupdated part within the same record, there is possibility that such failure cannot be detected.

[0026] To solve the above problem, it is necessary to provide a BCC in each record in the file area 121 of the storage unit 120. This results in that a large area is required for the BCCs, if a large volume of data need to be stored in the card.

[0027] As stated above, there has been developed no technique to repair and restore data failure (data recovery) within the IC card 100. If such repair and restore are handled on the side of the apparatus, the host computer needs to manage recovery information (restoration data and the like) of all IC cards every time the IC card is used. As a result, it is necessary to execute the recovery on data conflict by (1) communicating with the

host computer in real time to restore the data, or (2) prohibiting the IC card from being used, and issuing a new card.

[0028] To cope with the above problem, the conventional IC card has disadvantages such that a configuration of the IC card system become difficult, a large area is required to store recovery information in the storage of the host computer, and management of the entire IC card system becomes quite complex, as same as the PIN management. Further, to repair and restore the data in the IC card 100 in the event of a system failure, it is necessary to use a terminal apparatus accessible to the host computer, or to reissue the IC card. Such data recovery work is quite troublesome to the card user.

[0029] EP 0 583 006 A2 describes an IC card with a hierarchical file structure. The IC card comprises a processing controller, RAM and non-volatile memory. The non-volatile memory stores plural files in a logical file structure with five levels. Level 1 has a master directory, one key file and one data file. Each of levels 2-5 has one or more directories, key files and data files. Each data file and key file are managed by the directory.

[0030] Each data file comprises a data area for storing data. Each data file further has an access condition controller which comprises an excess key box designation table and a logic conditions area. The logic conditions area further comprises a horizontal matching condition settings area and a vertical matching condition settings table. The values set in the excess conditions controller differ for each data file.

[0031] The excess key box designation table is usually set by the card distributor and designates the key box numbers at which stored key data (which correspond to PINs) requires verification. The vertical matching condition settings table is also usually set by the card distributor and sets the levels from which the key files are collected and can be used for checking.

SUMMARY OF THE INVENTION

[0032] From the above viewpoint, an object of this invention is to provide a card type storage medium and a card type storage medium issuing apparatus, in which management of PINs heretofore carried out by a host computer becomes dispensable, the PIN management in the entire system is simplified, and verification of a PIN in an event of an accident is easily and simply carried out so that inconvenience to users may be mitigated upon verification of the PIN.

[0033] The present application also discloses a card type storage medium which can detect reliably conflicting data developed due to a system failure without using a BCC, and to realize repair and restore of the conflicting data developed due to a system failure by and within the card itself, thereby simplifying the apparatus configuration and reducing inconvenience to the users upon restoring the data.

[0034] The present invention therefore provides a

card type storage medium comprising a storage unit having a file area holding data in each file as a unit and a directory area holding therein control information units each including a PIN of a data file in said file area in said storage unit on the basis of said control information units in said directory area in said storage unit, said control unit allowing an access process on a data file only when a PIN held in said control information unit in said directory area in said storage unit is in agreement with a PIN fed from outside, the improvement comprising a dedicated file being set in said file area in said storage unit, said dedicated file holding PINs of the data files held in said respective control information units in said directory area in said storage unit and file names of the data files such that the PIN and file name of each data file correspond to each other, another control information unit being set in said directory area in said storage unit, said control information unit holding a master PIN of said dedicated file.

[0035] According to the above card type storage medium of this invention, a dedicated file is provided in a file area in the storage unit to hold data including PINs and files names of the respective data files. It is, therefore, possible to manage the PINs retained in each card type storage medium by and within the card type storage medium itself. It is also possible to omit PIN management by the host computer, largely reducing a burden of the PIN management on the entire system.

[0036] As another aspect, the present invention also provides a card type storage medium issuing apparatus issuing the above card type storage medium comprising the storage unit and the control unit, said card type storage medium issuing apparatus comprising a data file creating means, in response to a data file creating command from outside, setting a control information unit for a data file including a PIN of said data file to create said data file in said file area in said storage unit according to said data file creating command, a PIN matching means, in response to a data file accessing command to gain an access to the data file created by said data file creating means from the outside, making a judgement as to whether the PIN of said data file to be accessed according to said data file access command held in said control information unit in said directory area in said storage unit is in agreement with a PIN included in said data file accessing command supplied from the outside, a data file accessing means executing an access process on the data file to be accessed when said PIN matching means judges that said two PINs are in .. agreement, a dedicated file creating means, in response to a dedicated file creating command from the outside, setting a control information unit for said dedicated file including a master PIN for said dedicated file to create said dedicated file in said file area in said storage unit according to said dedicated file creating command, a master PIN matching means, in response to a dedicated file access command to gain an access to said dedicated file created by said dedicated file creating means

from the outside, making a judgement as to whether the master PIN of said dedicated file held in said control information unit in said directory area in said storage is in agreement with a master PIN included in said dedicated file access command supplied from the outside, and a dedicated file access means executing an access process on said dedicated file when said master PIN matching means makes a judgement that the above two master PINs are in agreement, upon issuing said IC card, said dedicated file accessing means writing the PINs of the data files held in said respective control information units in said directory area in said storage unit into said dedicated file such that the PIN and file name of each data file corresponds to each other according to a dedicated file accessing command supplied from outside after said dedicated file creating means created said dedicated file.

[0037] In the above card type storage medium issuing apparatus of this invention, upon issuing the IC card, said dedicated file creation instructing means first transfers a dedicated file creating command. Said dedicated file access instructing means then generates a dedicated file access command including data including PINs and file names of the respective data files and transfers it to said card type storage medium, thereby setting a dedicated file holding data including the PINs and file names of the respective data files such that a PIN and file name of each data file correspond to each other in the file area in the storage unit of the card type storage medium. It is, therefore, possible to manage the PINs of each card type storage medium by and within the card type storage medium itself. The management of the PINs by the host computer thus can be omitted, largely reducing a burden to manage the PIN on entire system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0038]

FIG. 1 is a block diagram illustrating an aspect of this invention;

FIG. 2 is a block diagram illustrating another aspect of this invention;

FIG. 3 is a block diagram illustrating a card type storage medium which is not part of the invention as claimed;

FIG. 4 is a block diagram illustrating a card type storage medium which is not part of the invention as claimed;

FIG. 5 is a block diagram showing a card type storage medium and an issuing apparatus issuing the card type storage medium according to the first embodiment of this invention;

FIG. 6 is a block diagram showing a file structure in a storage unit of the card type storage medium according to the first embodiment;

FIG. 7 is an illustration of a typical hardware configuration of the card type storage medium issuing ap-

paratus according to the first embodiment;

FIG. 8 is a block diagram showing a card type storage medium which is not part of the invention as claimed;

FIG. 9 is a block diagram showing a file structure in a storage unit of a card type storage medium which is not part of the invention as claimed;

FIG. 10 is an illustration showing a content of data held in a recovery information unit of the card type storage medium which is not part of the invention as claimed;

FIG. 11 is a flow chart of an operation to obtain recovery information in the card type storage medium which is not part of the invention as claimed;

FIG. 12 is a flow chart of an operation to detect a system failure and restore data in the card type storage medium which is not part of the invention as claimed;

FIGS. 13A through 13C are illustrations of a content of data in the recovery information unit in order to explain an operation of the card type storage medium which is not part of the invention as claimed;

FIG. 14 is an illustration of a content of data in the recovery information unit in order to explain the operation of the card type storage medium which is not part of the invention as claimed;

FIG. 15 is an illustration of a content of data in the recovery information unit in order to explain the operation of the card type storage medium which is not part of the invention as claimed;

FIGS. 16A and 16B are illustrations of a content of data in the application area and the recovery information unit in order to explain the operation of the card type storage medium which is not part of the invention as claimed;

FIG. 17 is a block diagram showing a configuration of a typical IC card;

FIG. 18 is an illustration showing a state of data stored in an IC card when a system failure occurred.

FIG. 19 is an illustration showing a state of data stored in an IC card when a system failure occurred.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

(1) Description of Aspects of This Invention

[0039] FIG. 1 is a block diagram illustrating an aspect of this invention. In FIG. 1, reference numeral 1 denotes a card type storage medium. The card type storage medium 1 comprises a storage unit 2 and a control unit 3.

[0040] The storage unit 2 includes a file area 21 holding data in each file as a unit and a directory area 23 having a control information unit 231 to hold a PIN for each data file 22 in the file area 21 therein.

[0041] The control unit 3 is to manage the data files 22 in the file area 21 in the storage unit 2 on the basis of data held in the control information units 231 in the

directory area 23 in the storage unit 2. In this card type storage medium 1; only when the PIN held in the control information unit 231 in the directory area 23 in the storage unit 2 agrees with a PIN fed from outside, the control unit 3 permits the data files to be accessed.

[0042] In the file area 21 in the storage unit 2 of this card type storage medium 1, there is provided a dedicated file 24 to hold PINs and file names of the data files 22 such that each of the PIN corresponds to its file name of the data file 22 that is retained in the control information units 231 in the directory area 23 in the storage unit 2. Likewise, there is provided another control information unit 232 to hold a master PIN (i.e., a PIN that only the system manager knows) for the dedicated file 24 in the director area 23 in the storage unit 2.

[0043] It is possible to encipher the PINs of the data files 22 and hold them in the dedicated file 24.

[0044] In the card type storage medium shown in FIG. 1, the data of the PINs for the respective data files 22 and the corresponding file names are set in the dedicated file 24. The PINs in each card type storage medium are therefore managed by and within the card type storage medium itself. As a result, the management of the PINs by the host computer is dispensable.

[0045] The data in the dedicated file 24 cannot be read out without an input of the master PIN (that is known by only the system manager) held in the control information unit 232 in the directory area 23.

The enciphered PINs for the respective data files 22 in the dedicated file 24 can more effectively prevent the PINs for the respective data files 22 from being known by other persons except the system manager, if the master PIN gets to be known by the other person.

[0046] FIG. 2 is a block diagram illustrating another aspect of this invention. In FIG. 2, reference numeral 10 denotes a card type storage medium. The card type storage medium 10 has a similar configuration to the card type storage medium shown in FIG. 1, essentially comprising a storage unit 2 and a control unit 3.

[0047] The storage unit 2 has, as similar to that shown in FIG. 1, a file area 21 retaining data in each file as a unit and a directory area 23 including control information units 231 each retaining a PIN for a data file 22 in the file area 21 therein.

[0048] The control unit 3 is, as also similar to the one shown in FIG. 1, to manage the data files 22 in the file area 21 in the storage unit 2 on the basis of the data held in the control information units 231 in the directory area 23 in the storage unit. The control unit 3 shown in FIG. 2 is provided with a data file creating means 31, a PIN matching means 32, a data file accessing means 33, a dedicated file creating means 34, a master PIN matching means 35 and a dedicated file accessing means 36.

[0049] When receiving a data file creating command from the outside (i.e., a card type storage medium issuing apparatus 4 described later), the data file creating means 31 sets the control information unit 231 for the

data file 22 containing a PIN for the data file 22 in response to the data file creating command in order to create said data file 22 in the file area 21 in the storage unit 2.

[0050] When receiving a data file access command to gain an access to the data file 22 created by the data file creating means 31 from the outside, the PIN matching means 32 makes a judgement as to whether a PIN included in the above data file accessing command agrees with the PIN of the data file 22 to be accessed held in the control information unit 231 in the directory area 23 in the storage unit 2.

[0051] The data file accessing means 33 is to gain an access to the data file 22 to be accessed when a result of the matching carried out by the PIN matching means 32 is positive.

[0052] When receiving a dedicated file creating command from the outside (i.e., the card type storage means issuing apparatus 4 described later), the dedicated file creating means 34 sets a control information unit 232 for a dedicated file 24 including a master PIN (known only by the system manager) for the dedicated file 24 in the directory area 23 in the storage unit 2 in response to the dedicated file creating command in order to create the dedicated file 24 in the file area 21 in the storage unit 2.

[0053] When receiving a dedicated file access command to gain an access to the dedicated file 24 created by the dedicated file creating means 34 from the outside (i.e., the card type storage medium issuing apparatus 4 described later), the master PIN matching means 35 makes a judgement as to whether the master PIN of the dedicated file 24 retained in the control information unit 232 in the directory area 23 in the storage unit 2 agrees with a master PIN contained in the inputted dedicated file access command.

[0054] When a result of the matching between the above two master PINs carried out by the master PIN matching means 35 is positive, the dedicated file accessing means 36 allows an access to the dedicated file 24.

[0055] Upon issuing the card type storage medium 10 of this invention, the dedicated file creating means 34, to begin with, creates the dedicated file 24. The dedicated file access means 36 next writes PINs of the respective data files 22 retained in the control information in the directory area 23 in the storage unit 2 into the dedicated file 24 such that each of the PIN of the data file 22 corresponds to its file name, in response to the dedicated file access command supplied from the outside (the card type storage medium issuing apparatus 4, described later).

[0056] It is possible to encipher the PINs for the data files 22 and hold them in the dedicated file 24.

[0057] In FIG. 2, reference numeral 4 denotes the card type storage medium issuing apparatus. The card type storage medium issuing apparatus 4 issues the card type storage medium 10 (or a card type storage

medium 1) as described hereinbefore, comprising a data file creation instructing means 41, a data file access instructing means 42, a dedicated file creation instructing means 43 and a dedicated file access instructing means 44.

[0058] The data file creation instructing means 41 sets a control information unit 231 of the data file 22 including a PIN for the data file 22 in the directory area 23 in the storage unit 2. The data file creation instructing means 41 then generates a data file creating command including the PIN, and transmit the generated data file creating command to the card type storage medium 10 (i.e., the data file creating means 31) in order to create the data file 22 in the file area 21 in the storage unit 2.

[0059] The data file access instructing means 42 generates a data file access command including a PIN for the data file 22 to be accessed, and transmits the generated data file accessing command to the card type storage medium 10 (i.e., the PIN number matching means 32 and the data file access means 32) in order to get an access to the data file 22 created in the file area 21 in the storage unit 2.

[0060] The dedicated file creation instructing means 43 sets the control information unit 232 for the dedicated file 24 including a master PIN for the dedicated file 24 in the directory area 23 in the storage unit 2. The dedicated file creation instructing means 43 generates a dedicated file creating command including the master PIN, and transmits the generated dedicated file creating command to the card type storage medium 10 (i.e., the dedicated file creating means 34) in order to create the dedicated file 24 in the file area 21 in the storage unit 2.

[0061] The dedicated file access instructing means 44 generates a dedicated file access command including the master PIN for the dedicated file 24, and transmits the generated dedicated file access command to the card type storage medium 10 (i.e., the master PIN matching means 35 and the dedicated file accessing means 36) in order to gain an access to the dedicated file 24 created in the file area 21 in the storage unit 2.

[0062] In the card type storage medium issuing apparatus 4, the dedicated file creating means 43 transfers a dedicated file creating instructing command to the card type storage medium 10 when the card type storage medium 10 is issued. Thereafter, the dedicated file access instructing means 44 generates a dedicated file access command including data of file names and PINs of the respective data files 22, and transfers it to the card type storage medium 10 (i.e., the dedicated file access means 36) in order to write the PINs of the data files 22 such that the PIN of each data file 22 corresponds to its file name that is retained in the control information unit 231 in the directory area 23 in the storage unit 2.

[0063] It is possible that, upon verification of PINs of the card type storage medium, the dedicated file access instructing means 44 of the card type storage medium issuing apparatus 4 generates a dedicated file access command including a master PIN, and transfers it to

the card type storage medium 10 (i.e., the master PIN matching means 35 and the dedicated file accessing means 36) in order to read out data from the dedicated file 24 in the file area 21 in the storage unit 2 in the card type storage medium 10 to be verified.

[0064] When the data of the PIN and the file name of the data file 22 is read out from the dedicated file 24 in the card type storage medium 10 in response to the dedicated file accessing command from the dedicated file access instructing means 44 of the card type storage medium issuing apparatus 4, the data file access instructing means 42 generates a data file accessing command including the PIN read out, and transfers it to the card type storage medium 10 (i.e., the PIN matching means 32 and the data file access means 33) to give an instruction to the card type storage medium 10 to verify the correctness of the data file 22 corresponding to the PIN read out.

[0065] In the case where enciphered PINs of data files are held in the dedicated file 24, there are also provided an enciphering means enciphering the PINs of the data files 22 to be written into the dedicated file 24 in the card type storage medium 10 by the dedicated file access directing means 44, and a decoding means decoding the enciphered PINs of the data files 22 read out from the dedicated file 24 in the card type storage medium 10 from the dedicated file access instructing means 44.

[0066] In the card storage medium 10 set forth above in connection with FIG. 2, the data file creating means 31 sets a control information unit 231 for the data file 22 including a PIN in the directory area 23 in the storage unit 2 in response to a data file creating command from the card type storage medium issuing apparatus 4.

[0067] When receiving a data file accessing command to access a data file 22 created by the data file creating means 31 from the outside, the PIN matching means 32 makes a judgement as to whether the PIN included in the data file accessing command agrees with the PIN of the data file 22 (held in the control information unit 231 in the directory area 23) to be accessed.

[0068] When a result of the matching executed by the PIN matching means 32 is positive, the data file access means 33 allows an access to the data file 22 to be accessed.

[0069] In the card type storage medium 10, the dedicated file creating means 34 sets, upon issuing the card type storage medium, the control information unit 232 for the dedicated file 24 including the master PIN (i.e., the PIN known by only the system manager) in the directory area 23 in the storage unit 2, in response to the dedicated file creating command in order to create the dedicated file 24 in the file area 21 in the storage unit 2.

[0070] When receiving the dedicated file accessing command to gain an access to the dedicated file 24 created by the dedicated file creating means 34 from the card type storage medium issuing apparatus 4, the master PIN matching means 35 makes a judgement as to

whether a master PIN included in the dedicated file accessing command agrees with the master PIN (retained in the control information unit 232 in the directory area 23) of the dedicated file 24.

[0071] When a result of the matching executed by the master PIN matching means 35 is positive, the dedicated file access means 36 carries out an access process (that is, write/read) on the dedicated file 24.

[0072] When the card type storage medium 10 is issued, the dedicated file accessing means 36 writes a PIN and a file name of each data file into a dedicated file 24 in such a manner that the PIN and the file name correspond to each other in response to a dedicated file accessing command from the card type storage medium issuing apparatus 4 after the dedicated file creating means 34 has created the dedicated file 24.

[0073] In the above manner, data of the PIN and the file name of each data file 22 is written in the dedicated file 24 in the file area 21 in the storage unit 2 of the card type storage medium 10. The management of the PINs in each card type storage medium 10 is carried out by and within the card type storage medium 10 itself, management of the PINs by the host computer is thus dispensable.

[0074] The data in the dedicated file 24 cannot be read out without knowing the master PIN (the PIN known by only the system manager) retained in the control information unit 232 in the directory area 23.

[0075] Encipherment of the PINs of the data files 22 stored in the dedicated file 24 is more effective to prevent the PINs of the data files 22 from leaking outside as they are, even if the master PIN gets to be known by another person except the system manager.

[0076] The above mentioned card type storage medium issuing apparatus 4 shown in FIG. 2 issues the card type storage medium 10 (or a card type storage medium 1).

[0077] More specifically, the data file creation instructing means 41 generates a data file creating command including PINs of data files 22, and transfers it to the card type storage medium 10 (i.e., the data file creating means 31) to set the control information unit 231 for the data files 22 including the PINs for the respective data files 22 in the directory area 23 in the storage unit 2, in response to the data file creating command so that the data files 22 may be created in the file area 21 in the storage unit 2.

[0078] The data file access instructing means 42 generates a data file accessing command including a PIN for a data file 22 to be accessed, and transfers it to the card type storage medium 10 (i.e., the PIN matching means 32 and the data file accessing means 32) to perform an access process (i.e., write/read) on the data file 22 created in the file area 21 in the storage unit 2.

[0079] On the other hand, the dedicated file creation instructing means 43 generates a dedicated file creating command including a master PIN, and transfers it to the card type storage medium 10 (i.e., the dedicated file cre-

ating means 34) to set the control information unit 232 for the dedicated file 24 including the master PIN for the dedicated file 24 so that the dedicated file 24 is created in the file area 21 in the storage unit 2.

[0080] The dedicated file access instructing means 44 generates a dedicated file accessing command including the master PIN for the dedicated file 24, and transfers it to the card type storage medium 10 (i.e., the master PIN matching means 35 and the dedicated file access means 36) to perform an access process (i.e., write/read) on the dedicated file 24.

[0081] Upon issuing the card type storage medium 10 (or the card type storage medium 1), the dedicated file creation instructing means 43, to begin with, transfers the dedicated file creating command. The dedicated file access instructing means 44 next generates a dedicated file accessing command including data of the PINs and the file names of the respective data files 22, and transfer it to the card type storage medium 10 (i.e., the dedicated file accessing means 36).

[0082] The data of the PINs and the file names of the respective data file 22 is set in the dedicated file 24 in the file area 21 in the storage unit 2 of the card type storage medium 10. The management of the PINs in the card type storage medium 10 is carried out by and within each card type storage medium 10 itself, the management of the PINs by the host computer may thus be omitted.

[0083] The data in the dedicated file 24 cannot be read out by a person not knowing the master PIN (i.e., the PIN known only by the system manager) retained in the control information unit 232 in the directory area 23.

[0084] In the event of an accident, the dedicated file access instructing means 44 generates a dedicated file access command including the master PIN, and transfers it to the card type storage medium 10 (i.e., the master PIN matching means 35 and the dedicated file accessing means 36), whereby the card type storage medium issuing apparatus 4 can read out the data (i.e., the data of the PINs and the file names of the respective data files 22) from the dedicated file 24 in the file area 21 in the storage unit 2 of the card type storage medium 10 to verify the PINs of the card type storage medium 10.

[0085] When the data of the PINs and the file names of the data files 22 is read out from the dedicated file 24 in response to the dedicated file accessing command from the dedicated file access instructing means 44, the data file access instructing means 42 generates a data file accessing command including the PIN read out, and transfers it to the card type storage medium 10 (i.e., the PIN matching means 32 and the data file accessing means 33) to verify the correctness of the data file 22 corresponding to the PIN.

[0086] It is possible to encipher PINs of the data files to be written in the dedicated file 24 by the dedicated file access instructing means 44, and decipher the enciphered PINs read out from the dedicated file 24 by the dedicated file access instructing means 44. The dedi-

cated file can therefore hold the enciphered PINs for the respective data files 22. If the master PIN is known by another person except the system manager, the enciphered PINs of the data files are securely prevented from being known as they are.

[0087] According to this invention, since the PINs of the data files 22 and their file names are held in the dedicated file 24 in the file area 21 in the storage unit 2 of the card type storage medium 1 or 10 in such a manner that the PIN and the file name of each data file 22 correspond to each other, as stated above. Therefore, each card type storage medium 1 or 10 can manage the PINs by and within the card type storage medium itself, the management of the PINs by the host computer becomes thus dispensable and the burden to manage the PINs in the entire system can be largely reduced.

[0088] The data in the dedicated file 24 is exhibited to be read out without use of the master PIN known by only the system manager. Moreover, the enciphered PINs of the respective data files 22 held in the dedicated file 24 can be effectively prevented from being known as they are by the other person, even if the master PIN gets to be known by the other person except the system manager. In which case, it is impossible to decipher the enciphered PINs as long as the manner of the encipherment is in secret. This can surely prevent the PINs from leaking outside, causing no trouble in security, even if the card type storage medium 1 or 10 manages the PINs therein.

[0089] Also according to this invention, when the card type storage medium issuing apparatus 4 issues the card type storage medium 1 or 10, the dedicated file creation instructing means 43 transfers a dedicated file creating command, the dedicated file access instructing means 44 then generates a dedicated file accessing command including data of the PINs and file names of the respective data files 22 to transfer it to the card type storage medium 1 or 10, whereby a dedicated file 24 holding the PINs and the file names of the respective data files 22 therein can be set so that the card type storage medium 1 or 10 can manage the PIN by itself. This can omit the management of the PINs by the host computer, largely simplifying the PIN management in the entire system. The data in the dedicated file 24 cannot be read out without the master PIN known by only the system manager.

[0090] In order to read out data of the PINs and the file names of the data files 22 from the dedicated file 24 of the card type storage medium 1 or 10, the dedicated file access instructing means 44 generates a dedicated file accessing command including the master PIN, and transfers it to the card type storage medium 1 or 10. In the event of an accident, it is possible to verify the PINs in the card type storage medium 1 or 10, mitigating inconvenience to the user upon verification of the PINs.

[0091] On the verification of a PIN, the data file access instructing means 44 transfers a data file accessing command to the card type storage medium in order to

verify the PIN read out from the dedicated file 24. This process make it possible to verify the correctness of the data file 22 corresponding to the PIN read out, with a high reliability in the PIN verification process.

[0092] The PINs to be written into the dedicated file 24 by the dedicated file access instructing means 44 are enciphered by the enciphering means, while the enciphered PINs read out from the dedicated file 24 by the dedicated file access instructing means 44 are enciphered by the enciphering means, whereby the dedicated file 24 can hold the PINs for the respective data file 22 as ciphers. If the master PIN gets to be known by person except the system manager, it is possible to prevent the PINs of the data files from leaking out as they are. So long as the manner of the encipherment does not leak out, it is impossible to decipher the PINs. This can prevent, with certain, the PINs from leaking outside, causing no trouble in security, even if the card type storage medium 1 or 10 manages the PIN therein.

[0093] In FIG. 3, reference numeral 11 denotes a card type storage medium, comprising a storage unit 2 and a control unit 5.

[0094] The storage unit 2 has a file area 21 holding data by files therein and a directory area 23 holding control information about each data file 22 in the file area 21 therein. The control unit 5 manages data in the file area 21 in the storage unit 2 on the basis of the control information in the directory area 23 in the storage unit 2. In the card type storage medium 11, the control unit 5 updates the objective data file 22 when receiving a command from outside.

[0095] The card type storage medium 11 is additionally provided a recovery information unit 25 in the data file 22 in the file area 21 in the storage unit 2, into which recovery information obtained every time an updating operation is performed on the objective data file 22 by the control unit 5 is written. In the recovery information unit 25, there are written (1) a start serial number obtained when the objective data file 22 is opened, (2) restoration data consisting of a record number to be updated and unupdated data at the record number obtained when the data file is updated, and (3) an end serial number obtained when the data file 22 is closed.

[0096] Meanwhile, it is possible to attach check serial numbers as recovery information, before and after the start serial number, the restoration data and the end serial numbers, respectively, in the recovery information unit 25.

[0097] If the updating process is performed a plurality of times on the same record number in the course from an open to close of the objective data file 22, the restoration data is not written into the recovery information unit 25 after the second updating process and later.

[0098] It is also possible to set information about a presence of the recovery information unit 25 in the objective data file 22 and information about a relative position of the recovery information unit 25 in the objective data file 22, if the recovery information unit 25 exists, in

the control information unit in the directory area 23 in the storage unit 2.

[0099] In the card type storage medium shown in FIG. 3, (1) a start serial number obtained when an objective data file 22 is opened, (2) restoration data consisting of a record number to be updated and unupdated data at the record number obtained when the objective data file 22 is updated, and (3) an end serial number obtained when the objective data file 22 is closed, are written as recovery information into the recovery information unit 25 additionally provided in the data file 22 in the file area 21 in the storage unit 2.

[0100] The start serial number in the recovery information unit 25 is compared with the end serial number. If a result of the comparison is in disagreement, it is possible to know from the result an occurrence of a system failure between an open and close of the objective data file 22, without using a BCC.

[0101] Moreover, the check serial numbers are attached before and after the start serial number, the restoration data and the end serial numbers, respectively, in the recovery information unit 25 as recovery information. The check serial numbers attached before and after the start serial number, the recovered number and the end serial number are compared with each other, respectively. If a result of the comparison is in disagreement, it is also possible to detect an occurrence of system failure in the course of writing the recovered data or the end serial number into the recovery information unit 25 so as to know the effectivity of each data stored in the recovery information unit 25.

[0102] If the same record number is updated plural times between an open and close of the objective data file 22, the restoration data obtained is not written into the recovery information unit 25 after the second updating process and later. It is therefore possible to always hold a preceding data (data before the updating) before the open of the data file 22 as restoration data at the same record number in the recovery information unit 25.

[0103] The above process enables the state inside the card type storage medium 11 after an occurrence of system failure to be effectively recovered to the state before the updating process where the system failure occurred.

[0104] By setting information as to the presence of the recovery information unit 25 in a data file and information about a relative position of the recovery information unit 25 in the objective data file 22, if the recovery information unit 25 exists, in the directory area 23 in the storage unit 2, it is possible to make a judgement as to whether a predetermined data should be written into the recovery information unit 25 or data recovery should be executed on the basis of the data stored in the recovery information unit 25.

[0105] In FIG. 4, reference numeral 12 denotes a card type storage medium corresponding to the second invention. The card type storage medium 12, as similar to the card type storage medium 11 shown in FIG. 3, es-

sententially comprises a storage unit 2 and a control unit 5.

[0106] The storage unit 2, as similar to the storage unit 2 shown in FIG. 3, has a file area 21 holding data in each file as a unit, and a directory area 23 holding control information including PINs for data files 22 in the file area 21 therein. In the data file 22 in the file area 21 in the storage unit 2 of this invention, there is additionally provided a recovery information unit 25 holding recovery information therein obtained every time the control unit 5 executes an updating operation on the data file 22.

[0107] The control unit 5 manages the data files 22 in the files area 21 in the storage unit on the basis of the control information in the directory area 23 in the storage unit 2, similarly to the one shown in FIG. 3. The control unit 5 includes a data file opening means 51, a data file updating means 52, a data file closing means 53, a start serial number obtaining means 54, a restoration data obtaining means 55 and an end serial number obtaining means 56.

[0108] When receiving an opening command from the outside, the data file opening means 51 opens a data file in the file area 21 in the storage unit 2 on the basis of the control information stored in the directory area 23 in the storage unit 2, in response to the opening command.

[0109] When receiving an updating command from the outside after the data file 22 has been opened, the data file updating means 52 updates data in the data file 22 that has been opened by the data file opening means 51.

[0110] When receiving a closing command from the outside after the data file 22 has been opened, the data file closing means 53 closes the data file 22 that has been opened by the data file opening means 51.

[0111] The start serial number obtaining means 54 obtains a start serial number when the data file 22 is opened by the data file opening means 51, and writes it as recovery information into the recovery information unit 25.

[0112] When the data file 22 is updated by the data file updating means 52, the restoration data obtaining means 55 obtains restoration data that is data before execution of the updating operation by the data file updating means 52, and writes it as recovery information into the recovery information unit 25.

[0113] The end serial number obtaining means 56 obtains an end serial number when the data file closing means 53 closes the data file 22, and writes it as recovery information into the recovery information unit 25.

[0114] Incidentally, it is possible to attach check serial numbers as recovery information before and after a start serial number, recovery data and end serial number, respectively, when the start serial number obtaining means 54, the recovery data obtaining means 55 and the end serial number obtaining means 56 obtain the start serial number, the restoration data and the end serial number, respectively, then write them together into the recovery information unit 25.

[0115] It is also possible to provide in the control unit 5 a restoration data initializing means initializing the restoration data obtained in the last process stored in the recovery information unit 25 before writing the new restoration data obtained this time by the recovery data obtaining means 55 into the recovery information unit 25.

[0116] When the data file updating means 52 carries out updating process a plurality of times on the same record number between an open and close of the objective data file 22, the recovered data obtaining means 55 does not write the restoration data into the recovery information unit 25 after the second updating and later.

[0117] It is also possible to set information about the presence of the recovery information unit 25 in data file 22 and information about a relative position of the recovery information unit 25 in the data file 22, if the recovery information unit 25 exists, in the control information unit for the data file 22 in the directory area 23 in the storage unit 2.

[0118] It is also possible to provide a failure detecting means in the control unit 5, which detects a failure in the last process, on the basis of a start serial number, an end serial number and check serial numbers attached before and after the start serial number and the end serial number, respectively, as recovery information stored in the recovery information unit 25, by referring to the control information about an objective data file in the directory area 23 in the storage unit 2 if the data file 22 has the recovery information unit 25, in response to an opening command from the outside.

[0119] If the check serial numbers attached before and after the start serial number are in disagreement, the failure detecting means judges that a failure occurred when the data file was opened by the data file opening means 51 in the last process. When detecting a failure that occurred when the data file was opened in the last process, the failure detecting means outputs a demand to perform once more the last process and a demand to restore the start serial number.

[0120] It is possible to provide a start serial number restoring means in the control unit 5, which restores the start serial number stored in the recovery information unit 25 to the one at the time of two updating processes earlier in response to the demand to restore the start serial number from the failure detecting means.

[0121] In the case where the check serial numbers attached before and after the start serial number are in agreement but the check serial numbers attached before and after the end serial numbers are in disagreement, the failure detecting means judges that a failure occurred when the data file was closed by the data file updating means 52 in the last process. When detecting that a failure occurred when the data file was closed in the last process, the failure detecting means outputs a demand to restore the end serial number.

[0122] It is possible to provide an end serial number restoring means in the control unit 5, which restores the end serial number stored in the recovery information unit

25 to the one at the time of the last process in response to a demand to restore the end serial number from the failure detecting means.

[0123] In the case where the check serial number attached before and after the start serial number and the check serial numbers attached before and after the end serial numbers are individually in agreement but the start serial number and the end serial number are in disagreement, the failure detecting means judges that a failure occurred in the course of updating the data file by the data file updating means 52 in the last process. When detecting that a failure occurred in the course of updating the data file in the last process, the failure detecting means outputs a demand to once more perform the last process and a demand to restore the data in the data file 22.

[0124] It is possible to provide a data restoring means in the control unit 5, which restores the data in the data file 22 on the basis of the restoration data stored in the recovery information unit 25 in response to a demand to restore the data in the data file 22 from the failure detecting means.

[0125] The data restoring means comprises a restoration data effectiveness detecting means which makes a judgement that the restoration data is effective when the check serial numbers attached before and after the restoration data are in agreement, and a restoration data writing means which, when the recovered data effectiveness detecting means judges that the restoration data is effective, writes said restoration data before the updating as data at the record number of said restoration data in the data file 22 into the data file 22.

[0126] In the card type storage medium 12 shown in FIG. 4, recovery information obtained every time the data file 22 is updated according to an instruction from the control unit 5 is written in the recovery information unit 25, which is provided in the data file 22 in the file area 21 in the storage unit 2.

[0127] More specifically, a start serial number obtained by the start serial number obtaining means 54 when the data file opening means 51 opens the data file 22, restoration data consisting of a record number to be updated and unupdated data at the same record number obtained by the restoration data obtaining means 55 when the data file updating means 52 updates the data file 22, and an end serial number obtained by the end serial number obtaining means 56 when the data file closing means 53 closes the data file 22 are written in the recovery information unit 25.

[0128] The start serial number and the end serial number in the recovery information unit 25 are compared with each other. If the two numbers are in disagreement, it means that a system failure occurred between an open and close of the data file 22. It is thus possible to detect a system failure without using a BCC.

[0129] When the start serial number obtaining means 54, the restoration data obtaining means 55 and the end serial number obtaining means 56 obtain a start serial

number, restoration data and an end serial number, respectively, check serial numbers are attached before and after the start serial number, the restoration data and the end serial number, respectively, then written into the recovery information unit 25 as recovery information. If the check serial numbers of the start serial number, the recovered data and the end serial number are in disagreement when compared with each other, it means that a system failure occurred while the start serial number, the recovered data or the end serial number are written into the recovery information unit 25 so that it becomes possible to detect a system failure and to verify the effectiveness of data stored in the recovery information unit 25.

[0130] Before the restoration data obtained by the restoration data obtaining means 56 is written into the recovery information unit 25, the restoration data obtained in the last process stored in the recovery information unit 25 is initialized by the recovery data initializing means, thereby preventing the previously stored restoration data from remaining in the recovery information unit by overwriting the new restoration data obtained in this process when the recovered data is written into the recovery information unit 25, further preventing an erroneous detection of a system failure or the like.

[0131] In the case where the updating process is carried out a plurality of times by the data file updating means 52 on the same record number between an open and close of the data file 22, the recovered data obtaining means 55 does not write the recovered data into the recovery information unit 25 after the second updating process and later. Whereby, the previous data obtained before the open of the data file 22 (data before the updating process) of the same record number may be always held as restoration data in the recovery information unit 25.

[0132] It is possible to restore the state of the card type storage medium 12 after a system failure has occurred to the state before an updating process in which the system failure occurred, on the basis of the data in the recovery information unit 25.

[0133] By setting information about the presence of the recovery information unit 25 and information about a relative position of the recovery information unit 25 in a data file 22, if the recovery information unit 25 exists, in the directory area 23 in the storage unit 2, it is possible to make a judgement as to whether predetermined data should be written into the recovery information unit 25 or data recovery on the basis of the data in the recovery information unit 25 should be performed, only by referring to the directory area 23 in the storage unit from the control unit 5.

[0134] In response to an opening command from the outside, the control information stored in the directory area 23 in the storage unit 2 with respect to the objective data file 22 is referred to. If the objective data file 22 has a recovery information unit 25, the failure detecting means provided in the control unit 5 checks as to wheth-

er a failure occurred in the last process or not, on the basis of a start serial number, an end serial number and check serial numbers attached before and after the start serial number and the end serial number, thereby detecting conflicting data having developed due to a system failure without using a BCC.

[0135] If the check serial numbers attached before and after the start serial number are in disagreement, the failure detecting means detects an occurrence of a failure when the data file was opened by the data file opening means 51 in the last process. When detecting a failure, the failure detecting means outputs a demand to execute once more the last process and a demand to restore the start serial number, thereby appropriately performing again the last process that was erroneously terminated due to the system failure.

[0136] The start serial number recovering means restores the start serial number stored in the recovery information unit 25 to the one at the time of the last process so that the state of the recovery information unit 25 can be automatically restored to the state at the time of two updating process earlier within the card type storage medium 12.

[0137] In the case where the check serial numbers attached before and after the start serial number are in agreement but the check serial numbers attached before and after the end serial number are in disagreement, the failure detecting means judges that a failure occurred when the data file closing means closed the data file in the last process. If detecting a failure, the failure detecting means outputs a demand to restore the end serial numbers to cause the end serial number restoring means to restore the end serial number stored in the recovery information unit 25 to the one at the time of the last process, thereby automatically restore the state of the recovery information unit 25 to the state at the time of the last process within the card type storage medium 12.

[0138] In the case where the check serial numbers attached before and after the start serial number and the check serial numbers attached before and after the end serial number are individually in agreement but the start serial number and the end serial number are in disagreement, the failure detecting means judges that a failure occurred during the last updating process carried out by the data file updating means 52. The failure detecting means outputs a demand to perform once more the last process and a demand to restore the data in the data file 22, thereby once again carrying out the last process that resulted in unsuccess due to the system failure.

[0139] The data restoring means restores the data in the data file 22 on the basis of the recovered data stored in the recovery information unit 25. This enables the data file 22 to be automatically restored to the state at the time of the two updating processes earlier (a state before the failure occurred), thereby once more executing the last process appropriately on the data file 22 in the

state two updating processes earlier.

[0140] When the data restoring means restores the data, the restoration data writing means writes only effective restoration data whose check serial numbers attached before and after the restoration data are judged by the restoration data effectiveness detecting means, thereby enabling data recovery without using restoration data in which a system failure occurred during writing it (that is, data whose check serial numbers attached before and after the data are in disagreement).

[0141] The start serial number and the end serial number in the recovery information unit 25 are compared with each other in the card type storage medium 11 or 12. If the start serial number and the end serial number are not in disagreement, it is thus possible to detect a system failure that occurred between an open and close of the data file 22. The check serial numbers attached before and after each data are also compared with each other. If the check serial numbers are in disagreement, it is thus possible to detect a system failure that occurred while a start serial number, recovered data or an end serial number are written into the recovery information unit 25, whereby the effectiveness of each data written in the recovery information unit 25 can be verified, further conflicting data developed due to the system failure can be surely detected.

[0142] Before the recovered data obtained by the recovery data obtaining means 55 is written in the recovery information unit 25, recovered data that was written in the recovery information unit 25 in the last process is initialized by the restoration data initializing means, thereby preventing the previous restoration data from remaining in the recovery information unit 25 by overwriting when the new restoration data is written in the recovery information unit 25, further preventing the system failure from being erroneously detected.

[0143] In the case where updating process is executed a plurality of times on the same record number by the data file updating means 52 between an open and close of the data file 22, the restoration data is not written in the recovery information unit 25 after the second updating and later. The recovery information unit 25 therefore can always hold data before the data file is opened (that is, data before the updating) at the same record number. It is thus possible, even after a system failure has occurred, to effectively restore the state in the card type storage medium 1 or 12 to a state before the updating process in which a system failure occurred, on the basis of the data in the recovery information unit 25.

[0144] Information about the presence of the recovery information unit 25 and information about a relative position of the recovery information unit 25 in the data file 22, if the recovery information unit 25 exists, are set in the directory area 23 in the storage unit 2, whereby a judgement can be made on as to whether predetermined data should be written into the recovery information unit 25, or data recovery should be performed on

the basis of the data in the recovery information unit 25, only by referring to the directory area 23 in the storage unit 2 from the control unit 5.

[0145] The failure detecting means can detect a failure having occurred in the last process on the basis of a start serial number, an end serial number and check serial numbers attached before and after the start serial number and the end serial number, respectively, held in the recovery information unit 25 in response to an opening command from the outside, if the data file 22 has the recovery information unit 25, thereby automatically detecting conflicting data developed due to a system failure without using a BCC within the card type storage medium 11 or 12.

[0146] According to a result of detection carried out by the failure detecting means, the start serial number restoring means, the end serial number restoring means, the data restoring means can automatically repair and restore the recovery information unit 25 or the application area, thereby simplifying the configuration of the system, reducing inconvenience to the users upon restoring the data, in addition.

[0147] When the data restoring means restores the data, the restoration data writing means writes only effective restoration data, whose check serial numbers attached before and after the restoration data are judged to be in agreement by the restoration data effective detecting means, into the data file. This makes it possible to store only certain and effective data, avoiding use of restoration data in which a system failure occurred while the restoration data was being written.

(b) Description of First Embodiment

[0148] Description will be hereinafter made in detail of a first embodiment of this invention. Now, referring to FIG. 7, there is shown an IC (integrated circuit) card 6 as a card type storage medium, having an IC unit 60 therein. The IC card 6 is issued by a card issuing apparatus (a card type storage medium issuing apparatus) 7 having a hardware configuration as shown in FIG. 7.

[0149] The IC card issuing apparatus 7 comprises, as shown in FIG. 7, an IC card reader/writer 71, a personal computer 72 and a printer 73.

[0150] The IC card reader/writer 71 is connected to the personal computer 72 via a dedicated line (for example, RS232C cable), into which the IC card 6 is inserted to be read out or written into.

[0151] The personal computer 72 causes the IC card reader/writer 71 to write data into the IC card 6 so that the IC card may have a predetermined data content therein, functioning as a main frame of the card issuing apparatus.

[0152] The printer 73 is served to printout a PIN and the like that is a result of verification made on personal identification numbers (PINs) onto a predetermined printing paper 75 in response to an instruction from the personal computer 72.

[0153] An internal configuration of the IC card 6 as a card type storage medium according to the first embodiment of this invention will be hereinafter described referring to FIGS. 5 and 6.

[0154] As shown in FIG. 5, the IC card 6 according to the first embodiment comprises a data communication mechanism 61, a storage unit 62 and a control unit 63.

[0155] The data communication mechanism 61 of the IC card 6 sends and receives information to and from the card issuing apparatus 7 when the IC card 6 is inserted into the IC card reader/writer 72 (or another terminal apparatus, a host computer, etc.) of the card issuing apparatus 7, including a terminal (a contact) which contacts with a terminal (of a data communication mechanism 710) of the IC card reader/writer 71 to transmit and receive signals thereto and therefrom.

[0156] The storage unit 62, employing a tree structure, includes a file area 621 including data to be processed by various application programs (i.e., programs to be incorporated in a terminal apparatus, a host computer, etc.) by files therein, and a directory area 623 holding control information about each file in the file area 621 therein.

[0157] For instance, data files (in an application using area) 622-1, 622-2, ..., to be handled by various application programs are held in the file area 621 in the storage unit 62, as shown in FIG. 6.

[0158] In this embodiment, the data file 622-1 is to be processed by an application program for cashless service, dedicated to hold data about, for example, the balance, use record, etc. therein. The data file 622-2 is to be processed by an application program for medical examination service in hospital or the like, dedicated to hold, for example, examination record, blood type, etc. therein.

[0159] The directory area 623 contains control information units 623-1, 623-2, ... about the respective data files 622-1, 622-2, ... therein.

[0160] In each of the control information units 623-1, 623-2, ..., a file name (APL-1 or APL-2), a position (a point or an address) in the file area 621, and a PIN (PIN; ABCD, or EFGH) of each of the data files 622-1, 622-2, ... are written.

[0161] The IC card 60 also has a dedicated file (different from the data files 622-1, 622-2, ..., for the application programs) in the file area 621 in the storage unit 62, used to manage PINs of the data files 622-1, 622-2, ..., retained therein, as shown in FIG. 6.

[0162] The dedicated file 624 holds data of file names (APL-1, APL-2, ...) of the data files (622-1, 622-2, ...) and their PINs (ABCD, EFGH, ...) in an enciphered form (PIN:****, #####, ...) in such manner that the each enciphered PIN of a data file corresponds to its file name.

[0163] The directory area 623 in the storage unit 62 has a control information unit 623-0 for the dedicated file 24, in which a position (a point or an address) in the file area 621, a file name (Master), and a master personal identification number (a PIN known by only the

system manager, hereinafter referred, occasionally, as a master PIN) of the dedicated file 624 are held.

[0164] As shown in FIG. 5, the control unit (MPU: micro processor unit) 63 of the IC card 6 is to manage data retained in the file area 621 in the storage unit 62 according to the control information held in the directory area 623 in the storage unit 62. The control unit 63 according to this embodiment, comprises a data file creating unit 631, a PIN matching unit 632, a data file accessing unit 633, a dedicated file creating unit 634, a master PIN matching unit 635 and a dedicated file accessing unit 636.

[0165] The data file creating unit 631 sets the control information units 623-1, ... including pins, points and files names of the respective data files 622-1, ... in the directory area 623 in the storage unit 62 in response to a data file creating command from the card issuing apparatus 7 to create the data files 622-1, ... in the file area 621 in the storage unit 62.

[0166] In response to a data file access command from outside (i.e., the card issuing apparatus 7, the terminal apparatus, the host computer, etc.) to access a data file 622-1 created by the data file creating unit 631, the PIN matching unit 632 makes a judgement as to whether a PIN of the data file 622-1, ... that is an object of the access command (i.e., a PIN held in the control information unit 623-1 in the directory area 623) is in agreement with a PIN fed from the outside included in the above data file access command.

[0167] The PIN matching unit 632 according to this embodiment also has a file locking function to lock a data file 622-1, ... that is an object of an access when the matching of the PINs is successively resulted in failure predetermined times, and a function to release the file locking state in response to an instruction from the outside, in addition to the above matching function.

[0168] The data file access unit 633 executes an access process (write/read) on the data file 622-1 that is an object of the access when the PIN matching unit 632 judges that the PINs are in agreement.

[0169] The dedicated file creating unit 634 sets a control information unit 623-0 including a master PIN, a point and a file name of a dedicated file 624 in the directory area 623 in the storage unit 62 in response to a dedicated file creating command from the card issuing apparatus 7 to create the dedicated file 624 in the file area 621 in the storage unit 62.

[0170] In response to a dedicated file access command from the card issuing apparatus 7 to gain an access to the dedicated file 624 created by the dedicated file creating unit 634, the master PIN matching unit 635 makes a judgement as to whether a master PIN held in the control information unit 623-0 in the directory area 623 is in agreement with a master PIN included in the above dedicated file access command from the card issuing apparatus 7.

[0171] When the master PIN matching unit 635 judges that the two PINs are in agreement, the dedicated file

access unit 636 executes an access process (write/read) on the dedicated file 624.

[0172] At the time of issuing the IC card 6, the dedicated file creating unit 634, to begin with, creates the dedicated file 624, the dedicated file access unit 636 next writes PINs (enciphered PINs in this embodiment) and file names of the respective data files 622-1, ... into the dedicated file 624 such that each PIN of the data file corresponds to its file name, in response to a dedicated file access command supplied from the card issuing apparatus 7.

[0173] The IC card may have an electric source therein, or may be supplied electric energy from the card issuing apparatus 7, the terminal apparatus or the host computer when the IC card is inserted into them. In the latter case, a non-volatile storage such as an EEPROM is employed to the storage unit 62 of the IC card 6.

[0174] A configuration of the card issuing apparatus 7 which issues a card type storage medium according to the first embodiment will be next described in detail, referring to FIG. 5.

[0175] As stated above in connection with FIG. 7, the card issuing apparatus 7 according to the first embodiment comprises the IC card reader/writer 71, the personal computer 72 and the printer 73.

[0176] The IC card reader/writer 71 has the data communication mechanism 710 which is adapted to communicate between the IC card 6 and the personal computer 72 to write or read information to and from the IC card 6 when the IC card 6 is inserted thereinto. The data communication mechanism 710 includes a terminal (a contact) contacting with a terminal (of a data communication mechanism 61) of the IC card 6 to send or receive signals.

[0177] The personal computer 72 functions as a card issuing apparatus to issue the above IC card 6 as mentioned above, comprising a data file creation instructing unit 721, a data file access instructing unit 722, a dedicated file creation instructing unit 723, a dedicated file access instructing unit 724, an enciphering unit 725 and a decoding unit 726.

[0178] The data file creation instructing unit 721 sets control information units 623-1 including PINs, points, file names of respective data files 622-1, ... in the directory area 623 in the storage unit 62. In order to create the data files 622-1, ... in the file area 621 in the storage unit 62, the data file creation instructing unit 721 generates a data file creating command including control information such as the PINs of the data files on the basis of data file creating data (including the PINs) stored in the floppy disk 76, and transfers the generated data file creating command to the data file creating unit 631 of the IC card 6 via the data communication mechanisms 710 and 61.

[0179] The data file access instructing unit 722 generates a data file access command including a PIN for a data file 622-1 to be accessed in order to execute an access process on the created data file 622-1 in the file

area 621 in the storage unit 62 of the IC card 6, then transfers the generated data file access command to the IC card 6 (the PIN matching unit 632 and the data file access unit 632). The data file access instructing unit 722 also has a function to transfer an instruction to verify the correctness of the data file corresponding to the PIN when the PIN in the IC card 6 is checked, as described later.

[0180] The dedicated file creation instructing unit 723 sets a control information unit 623-0 including a master PIN, a point, a file name of the dedicated file 624 in the directory area 623 in the storage unit 62 of the IC card 6. In order to create the dedicated file 624 in the file area 621 in the storage unit 62 of the IC card 6, the dedicated file creation instructing unit 623 generates a dedicated file creating command including the master PIN on the basis of dedicated file creating data stored in the floppy disk 77, then transfers the generated dedicated file creating command to the dedicated file creating unit 634 of the IC card 6 via the data communication mechanisms 710 and 61.

[0181] In order to execute an access process on the dedicated file 624 created in the file area 621 in the storage unit 62 of the IC card 6, the dedicated file access instructing unit 724 generates a dedicated file access command including the master pin of the dedicated file 624, then transfers the generated dedicated file access command to both the master PIN matching unit 635 and the dedicated file access unit 636 of the IC card 6 via the data communication mechanisms 710 and 61. The dedicated file access instructing unit 624 also has a function to transfer an instruction to verify the PINs of the IC card 6, as described later.

[0182] The dedicated file access instructing unit 724 according to this embodiment also has a function to generate a dedicated file access command including data, a pair of the enciphered PIN and the file name of each data file 622-1, ..., on the basis of the data file creating data stored in the floppy disk 76, then transfers the generated dedicated file access command to the dedicated file access unit 636 of the IC card 6 via the data communication mechanisms 710 and 61 upon issuing the IC card 6, after the dedicated file creation instructing unit 723 transferred the dedicated file creating command to the IC card 6.

[0183] The personal computer 72 of the card issuing apparatus 7 according to this embodiment is provided the enciphering unit 725 which enciphers the PINs of the data files 622-1, ... supplied from the floppy disk 76 in order to write the enciphered PINs of the data files 622-1 into the dedicated file 624, and the decoding unit 726 which deciphers the enciphered PINs read out from the dedicated file 624 when PIN verification is carried out, as described later.

[0184] Upon checking a PIN of the IC card 6, the dedicated file access instructing unit 724 according to this embodiment functions to generate a dedicated file access command including the master PIN in order to read

out data from the dedicated file 624 of the IC card 6 which holds therein the PIN to be verified, then transfer the generated dedicated file access command to both the master PIN matching unit 635 and the dedicated file access unit 636 via the data communication mechanisms 710 and 61.

[0185] When the data (that is, data of a pair of the enciphered PIN and the file name of the data file 622-1) is read out from the dedicated file 624 of the IC card 6 in response to the dedicated file access command from the dedicated file access instructing unit 724 upon verification of the PIN of the IC card 6, the data file access instructing unit 722 according to this embodiment generates a data file access command including the PIN read out (that is, the PIN deciphered by the decoding unit 726), then transfers the generated data file access command to both the PIN matching unit 632 and the data file access unit 633 via the data communication mechanisms 710 and 61 so as to give an instruction to the IC card 6 to verify the correctness of the data file 622-1 corresponding to the PIN read out.

[0186] The printer 73 has a PIN printing mechanism 78. When the data file access instructing unit 724 verifies the correctness of the PIN read out by the dedicated file access instructing unit 724 upon PIN verification, the PIN printing mechanism of the printer 73 printouts the PIN that is a result of the verification on a predetermined printing paper 75 in response to an instruction from the personal computer 7.

[0187] To issue the IC card 6 according to this embodiment, the following process is performed, with the IC card 6 being inserted in the IC card reader/writer of the card issuing apparatus 7.

[0188] The dedicated file creating instructing unit 723 converts the dedicated file creating data (including the master PIN) stored in the floppy disk 77 into data in a format for a program incorporated in the IC card 6 to generate a dedicated file creating command including the master PIN, then transfers the generated dedicated file creating command to the dedicated file creating unit 634 of the IC card 6 via the data communication mechanisms 710 and 61.

[0189] In the IC card 6, when receiving the dedicated file creating command, the dedicated file creating unit 634 sets a control information unit 623-0 including a master PIN, a point and a file name of the dedicated file 624 in the directory area 623 in the storage unit 62 in response to the dedicated file creating command so as to create the dedicated file 624 in the file area 621 in the storage unit 62.

[0190] The data file creation instructing unit 721 in the card issuing apparatus 7 converts the data file creating data (including PINs for a card owner) stored the floppy disk 67 into data in a format for a program incorporated in the IC card 6 to generate a data file creating command including the PINs, then transfers the generated data file creating command to the data file creating unit 631 of the IC card 6 via the data communication mecha-

nisms 710 and 61.

[0191] In the IC card 6, when receiving the data file creating command, the data file creating unit 631 sets a control information units 623-1 each including a PIN, a point and a file name of the data file 622-1 in the directory area 623 in the storage unit 62 in response to the data file creating command to create the data files 622-1 in the file area 621 in the storage unit 62.

[0192] Next, PINs are extracted from the data file creating data stored in the floppy disk in the card issuing apparatus 7, then enciphered to be an enciphered PINs. The dedicated file access instructing unit 724 then converts the data of a pair of the enciphered PIN and the file name of each data file 622-1 into data in a format for a program incorporated in the IC card 6 to generate a dedicated file access command including the above data, then transfers the generated dedicated file access command to the dedicated file access unit 636 of the IC card 6 via the data communication mechanisms 710 and 61.

[0193] When receiving the the dedicated access command, the dedicated file access unit 636 of the IC card 6 writes the enciphered PINs of the respective data files 622-1 in the dedicated file 624 such that the enciphered PIN of the data file 622-1 corresponds to its file name in response to the dedicated file access command, as shown in FIG. 6.

[0194] Through the above process, the IC card 6 is issued, going into a state to be able to receive general application services. At that time, the PINs for each card owner are managed in the dedicated file 624 in the IC card 6 that is possessed by the card owner.

[0195] To receive a general application service through the IC card, the owner inserts the IC card 6 into the terminal apparatus or the host computer providing the predetermined application. The terminal apparatus or host computer gives a data file access command to the IC card 6 to cause the IC card 6 to perform an access process (write/read) on each data file 622-1, ... in the storage unit 62.

[0196] More specifically, when receiving the data file access command from the terminal apparatus, host computer or the like, the PIN matching unit 632 makes a judgement as to whether a PIN of the data file 622-1 to be accessed (held in the control information unit 623-1 in the directory area 623) is in agreement with a PIN included in the data file access command supplied from the outside (i.e., a PIN inputted by the card owner through the terminal apparatus, host computer or the like).

[0197] When the PIN matching unit 632 makes a judgement that the above two PINs are in agreement, the data file access unit 633 performs an access process (write/read) on the objective data file 622-1. When the PIN matching unit 632 successively draws the same conclusion predetermined times that the above two PINs are in disagreement, the PIN matching unit 632 locks the objective data file 622-1 so that the data file

622-1 is prohibited from being used.

[0198] Meanwhile, if the card owner forgets the PIN of his or her own IC card 6 after the issue of the IC card 6, it is possible to verify the PIN by carrying out the following process with the IC card 6 being inserted in card reader/writer 71 of the card issuing apparatus 6, according to this embodiment.

[0199] Namely, in order to read out data in the dedicated file 624 in the IC card 6, the dedicated file access instructing unit 724 generates a dedicated file access command including the master PIN, then transfers the generated dedicated file accessing command to both the master PIN matching unit 635 and the dedicated file access unit 636 of the IC card 6 via the data communication mechanisms 710 and 61.

[0200] On the side of the IC card 6, the master PIN matching unit 635 compares the master PIN (held in the control information unit 623-0 in the directory area 623) of the dedicated file 624 with the master PIN included in the dedicated file access command when receiving the dedicated file access command.

[0201] If the mater PIN matching unit 635 makes a judgement that the two master PINs are in agreement, the dedicated file accessing unit 636 reads out the data of a pair of the enciphered PIN and the file name of a data file from the dedicated file 624, then transfers it to the dedicated file access instructing unit 724 of the card issuing apparatus 7 via the data communication mechanisms 61 and 710.

[0202] The dedicated file access instructing unit 724 next makes the decoding unit 726 decipher the enciphered PIN, then reports data of a pair of the deciphered PIN and the file name of the data file to the data file access instructing unit 722.

[0203] When receiving the report form the dedicated file access instructing unit 724, the data file accessing instructing unit 722 generates a data file access command including the deciphered PIN, then transfers the generated data file accessing command to both the PIN matching unit 632 and the data file access unit 633 of the IC card 6 via the data communicating mechanisms verification on the correctness of the data file 622-1 corresponding to the PIN read out.

[0204] On the side of the IC card 6, the PIN matching unit 632 checks as to whether the PIN (held in the control information unit 623-1 in the directory area 623) of the data file 622-1 to be verified is in agreement with the PIN included in the data file accessing command supplied from the card issuing apparatus 7, in response to the data file accessing command to verify the correctness of the PIN.

[0205] If the PIN matching unit 632 draws a conclusion that the two PINs are in agreement, it is judged that the correctness of the data file 622-1 corresponding to the PIN read out has been verified. At that time, if the data file 622-1 that is an object of the correctness verification is in a locked state, the PIN matching unit the IC card 6 into a normal state.

[0206] When the correctness of the IC card 6 is verified in the above manner, the PIN printing mechanism 78 of the printer 73 printouts the deciphered PIN read out by the dedicated file access instructing unit 724 on the predetermined printing paper 75, then the verification of the PIN finishes.

[0207] According to the first embodiment, the data consisting of a pair of the PIN and file name of each data file 622-1, ... is set in the file area 621 in the storage unit 62 of the IC card 6. The PINs in each IC card 6 are managed by and within the IC card itself, without need for management of the PINs by the host computer, thereby largely reducing a burden for PIN management on the entire IC card system.

[0208] The data in the dedicated file 624 cannot be read out without the master PIN known by only the system manager. Even if the master PIN leaked out except the system manager, the PINs of the data files 622-1, ... do not leak out as they are, since each of the PIN of the data file 622-1 is enciphered. So long as the manner to encipher the PINs of the data files 622-1 is kept in secret, each PIN cannot be solved.

[0209] It is therefore possible to securely prevent the PINs from being out and avoid a problem in security, even if the PINs are managed by and within the IC card 6.

[0210] Further, upon verification of the PINs in the case of an accident, the dedicated file access instructing unit 724 of the card issuing apparatus 7 generates a dedicated file accessing command including the master PIN, then transfers the command to the IC card 6. The manner of this verification is quite simple and can reduce inconvenience to the card user.

[0211] According to this embodiment, when the PIN is verified, the data file access instructing unit 722 transfers a data file accessing command to the IC card 6 to verify the correctness of the PIN read out from the dedicated file 624, and the PIN matching unit 632 executes a PIN matching to make sure the correctness of the data file 622-1 corresponding to the PIN read out, thereby increasing the reliability in the PIN verification.

[0212] In the above embodiment, the data file creating data and the dedicated file creating data are supplied from the floppy disks 76 and 77, respectively. It is also possible to input the data file creating data and the dedicated file creating data through a keyboard or the like.

(c) Description of a card type storage medium which is not part of the invention as claimed

[0213] Referring now to FIG. 8, an IC card 8 comprises a storage unit 81 and a control unit 82.

[0214] The storage unit 81 has a tree structure, including a file area 811 holding data to be processed by various application programs (i.e., programs incorporated in a terminal apparatus, a host computer, etc.) by files therein, and a directory area 813 holding control information about each of data files 812 in the file area 811

therein.

[0215] In the directory area 813, a file name, a personal identification number (PIN), a position (i.e., and the like of each data file 812 held in the file area 811 are written.

[0216] The IC card 8 according to this embodiment is additionally provided with a recovery information unit 815 in the data file 812 in the file area 811 in the storage unit 81, into which the control unit 82 writes recovery information obtained every time the data file 812 is updated, as shown in FIG. 9.

[0217] More concretely, as shown in FIG. 10, record numbers #1 to #n are allocated to an application area 814 to store data to be processed by one of various application programs (i.e., data of the balance in the case of a cashless card), and record numbers after #n+1 and later are allocated to the recovery information unit 815.

[0218] As shown in FIG. 10, a start serial number (the number of processed items) obtained when the data file 812 is opened is written in the record number #n+1 in the recovery information unit 815, an end serial number (the number of processed items) obtained when the data file 812 is closed is written in the record number #n+2, and restoration data consisting of a record number whose data has been updated (i.e., an updated record number in the application area 814) and unupdated data at the same record number (i.e., data before subjected to the updating in the application area 814) obtained when the data file 812 is updated is written in the record numbers after #n+3 and later. According to this embodiment, check serial numbers (the number of items) are respectively attached, as recovery information, before and after the start serial number, the restoration data and the end serial number held in the recovery information unit 815.

[0219] As shown in FIG. 9, there are set, in the directory area 813 in the storage unit 81 as control information of each data file 812, information as to whether the recovery information unit 815 is additionally provided in a data file 812 (that is, information about the presence of the recovery information in a data file 812), information about a relative position of the recovery information unit 815 in the data file 812, if the recovery information 815 exists in the data file 812 (that is, the leading record number of the recovery information unit 815), and a size and a number of the recovery information unit 815.

[0220] The control unit 82 is adapted to manage the data files 812 in the file area 811 in the storage unit 81 on the basis of the control information held in the directory area 813 in the storage unit 81, comprising a data file opening unit 821, a data file updating unit 822, a data file closing unit 823, a start serial number obtaining unit 824, a restoration data obtaining unit 825, an end serial number obtaining unit 826, a restoration data initializing unit 827, a system failure detecting unit 828, a start serial number restoring unit 829, an end serial number restoring unit 830 and a data restoring unit 831.

[0221] When receiving an OPEN command (an open

instruction) from an application program 9 incorporated in a terminal apparatus or the like into which the IC card 8 is inserted, the data file opening unit 821 opens a data file 812 designated by the open command, on the basis of the control information in the directory area 813 in the storage unit 81.

[0222] When receiving a WRITE command (an updating instruction) from the application program 9 after the data file 812 has been opened, the data updating unit 822 updates data in the data file 812 having been opened by the data file opening unit 821.

[0223] When receiving a CLOSE command (a closing instruction) from the application program 9 after the data file 812 has been opened, the data file closing unit 823 closes the data file 812 having been opened by the data file opening unit 821.

[0224] The start serial number obtaining unit 824 obtains a start serial number (whose initial value is 0) by adding 1 to the latest start serial number when the data file 812 is opened by the data file opening unit 821. The start serial number obtaining unit 824 also attaches check serial numbers (whose initial value is 1, incremented by 1 every time the data file 812 is opened) before and after the start serial number, and writes both the start serial number and its check serial numbers as recovery information in the record number #n+1 of the recovery information unit 815.

[0225] The restoration data obtaining unit 825 acquires restoration data including a record number to be updated and unupdated data at the same record number when the data file 812 is updated by the data file updating unit 822. The restoration data obtaining unit 825 also attaches check serial numbers before and after the restoration data, and writes the restoration data and its check serial numbers as recovery information in the record number on and after #n+3, in order.

[0226] If the data file updating unit 822 executes plural times of updating process on the same record number between an open and close of the data file 812, the restoration data obtaining unit 825 does not write data into the recovery information unit 815 after the second updating process and later.

[0227] The end serial number obtaining unit 826 obtains an end serial number (whose initial value is 0) by adding 1 to the latest start serial number when data file closing unit 823 closes the data file 812. The end serial number obtaining unit 826 also attaches check serial numbers (whose initial values are 1, incremented by 1 every time the data file 812 is closed) before and after the end serial number, and writes both the end serial number and its check serial numbers as recovery information into the record number #n+2 in the recovery information unit 815.

[0228] Before the restoration data having been acquired by the restoration data obtaining unit 825 has been written into the recovery information unit 815, the restoration data initializing unit 827 initializes the restoration data that is being stored in the recovery informa-

tion unit 815 (more specifically, setting the restoration data all at 0 and the check serial numbers all at 1).

[0229] When receiving an OPEN command (an open instruction) from the application program 9, the system failure detecting unit (a failure detecting means) 828, firstly, looks up the control information relating to a data file 812 designated by the OPEN command held in the directory area 813 in the storage unit 81. If the data file 812 has a recovery information unit 815 therein, the system failure detecting unit 828 detects a failure having occurred in the last process on the basis of the start serial number, the end serial number and the check serial numbers attached before and after these start serial number and end serial number, respectively, written as recovery information in the recovery information unit, through following procedure shown in FIG. 12.

[0230] When the check serial numbers attached before and after the start serial number are in disagreement, the system failure detecting unit 828 makes a judgement that a failure occurred when the data file opening unit 821 opened the data file in the last process, outputting a demand to reprocess the last process to the application program 9 and a demand to restore the start serial number to the start serial number restoring unit 829.

[0231] When receiving a demand to restore the start serial number from the system failure detecting unit 828, the start serial number restoring unit 829 restores the start serial number stored in the recovery information unit 815 to the one at the time of two updating processes earlier.

[0232] When the check serial numbers attached before and after the start serial number are in agreement but the check serial numbers attached before and after the end serial number are in disagreement, the system failure detecting unit 828 makes a judgement that a failure occurred when the data file closing unit 823 closed the data file in the last process, and outputs a demand to restore the end serial number to the end serial number restoring unit 830.

[0233] When receiving the demand to restore the end serial number from the system failure detecting unit 828, the end serial number restoring unit 830 restores the end serial number being stored in the recovery information unit 815 to the one at the time of the last process.

[0234] When the check serial numbers attached before and after the start serial number and the check serial numbers attached before and after the end serial number are in agreement but the start serial number and the end serial number are in disagreement, the system failure detecting unit 828 judges that a failure occurred when the data file updating unit 822 updated the data file in the last process, and outputs a demand to perform once again the last process to the application program 9 and a demand to restore the data in the data file 812 to the data restoring unit 831.

[0235] When receiving the demand to restore the data in the data file 812 from the system failure detecting unit

828, the data restoring unit 831 restores the data in the application area 814 in the data file 812 on the basis of the restoration data stored in the recovery information unit 815.

[0236] The data restoring unit 831, according to this embodiment, comprises a restoration data effectiveness detecting unit 832 and a restoration data writing unit 833.

[0237] The restoration data effectiveness detecting unit 832 judges that the restoration data is effective when the check serial numbers attached before and after the restoration data are in agreement. The restoration data writing unit 833 writes the unupdated data of the restoration data having been judged to be effective by the restoration data effectiveness detecting unit 832 as the data at the record number of the above restoration data in the application area 814 of the data file 812.

[0238] According to this embodiment, the recovery information is acquired in the IC card 8 in a normal updating process instructed by the application program 9 through following procedure shown in FIG. 11.

[0239] When receiving an OPEN command from the application program 9, the system failure detecting unit 828 of the IC card 8 detects a failure that has occurred in the last process (Step S1).

[0240] If a system failure is not detected, or a system failure is detected and a recovery process (a data recovery process) is executed by the restoring unit 829-831, the restoration data initializing unit 827 initializes the restoration data that has been written in the recovery information unit 815 in the last process by setting all the restoration data at 0 and all the check serial numbers at 1 (Step S2). (Meanwhile, a manner for the system failure detecting and the data restoring will be described later, referring to FIG. 12.).

[0241] The start serial number obtaining unit 824 obtains a check serial number and a start serial number by adding 1 to the latest start serial number (whose initial value is 0) and the check serial numbers (whose initial value is 1), and writes the new start serial number and its check serial numbers attached before and after the start serial number as recovery information in the record number #n+1 in the recovery information unit 815 (Step S3).

[0242] Thereafter, the data file opening unit 821 opens the data file 812 designated by the open command on the basis of the control information in the directory area 813 in the storage unit 81 (Step S4).

[0243] After the data file 812 is opened, the restoration data obtaining unit 825 obtains restoration data including a record number to be updated and unupdated data at this record number every time the application program 9 supplies a WRITE command (an updating instruction), and writes the restoration data and its check serial numbers attached before and after the restoration data in the record number on and after #n+3 in the recovery information unit 815, in order (Step S5). In the case where the data file updating unit 822 executes the

updating process plural times on the same record number between an open and close of the data file 812, the restoration data will not be written into the recovery information unit 815 after the second updating process and later.

[0244] After the restoration data obtaining unit 825 has obtained the restoration data, the data file updating unit 822 updates the data in the data file 812 (Step S6).

[0245] While the application program 9 supplies a WRITE command (an updating instruction), the process in the steps S5 and S6 is repeated.

[0246] When receiving a close command from the application program 9, the end serial number obtaining unit 826 obtains an end serial number and its check serial numbers by adding 1 to the latest end serial number (whose initial value is 0) and the check serial numbers (whose initial value is 1) as same as in the step S3. The end serial number with the check serial numbers attached before and after the end serial number are written into the record number #n+2 in the recovery information unit 815 as recovery information (Step S7).

[0247] Thereafter, the data file closing unit 823 closes the data file 812 (Step S8).

[0248] In the above manner, the recovery information is written in the recovery information additionally provided in the data file 812 in the file area 811 in the storage unit 81 every time the control unit causes the data file 812 to be updated.

[0249] A manner to detect a system failure in the last process by the system failure detecting unit 828 and a restoring process (a data recovery process) when a system failure is detected in the IC card 8 carried out in Step 1 shown in FIG. 11 will be now described in more detail, referring to FIG. 12.

[0250] When receiving an OPEN command from the application program 9, a reference is made to the control information about a designated data file 812 in the directory area 813. If the data file 812 has a recovery information unit 815 therein, the system failure detecting unit 828 detects a system failure having occurred in the last process, on the basis of the recovery information (i. e., a start serial number, an end serial number and check serial numbers attached before and after the start serial number and the end serial number) stored in the recovery information unit 815.

[0251] Namely, a judgement is first made as to whether the check serial numbers attached before and after the start serial number are in agreement or not (Step S11). If the check serial numbers are in disagreement, it is judged that a system failure occurred when the data file was opened by the data file opening unit 821 in the last process, then a demand to reprocess the last process and a demand to restore the start serial number are outputted to the application program 9 and the start serial number restoring unit 829, respectively.

[0252] The start serial number restoring unit 829 restores the start serial number stored in the recovery information unit 815 to the one at the time of two updating

processes earlier (Step S12). Then in the step S2 shown in FIG. 11, the application program 9 once more carries out the process that should have been done in the last process in response to the reprocessing demand from the system failure detecting unit 828.

[0253] On this occasion, since a system failure occurred when the data file was opened in the last process, it can be assumed that no updating process has been performed on the data file 812, and thus the restore data and end serial number in the recovery information unit 815. Therefore, only the start serial number is restored to the one at the time of two updating processes earlier without carrying out the data restoring (data recovery), and a demand for the reprocessing is given to the application program 9. As this, the program of the last process can be appropriately executed in the recovery information unit 815.

[0254] If it is judged in the Step S11 that the check serial numbers attached before and after the start serial number are in agreement, the next judgement is made as to whether the check serial numbers attached before and after the end serial number are in agreement or not (Step S13). If the check serial number attached before and after the end serial number are in disagreement, it is judged that a failure occurred when the data file was opened by the data file opening unit 823 in the last process, and a demand to restore the end serial number is outputted to the end serial number restoring unit 830.

[0255] The end serial number restoring unit 830 then restores the end serial number stored in the recovery information unit 815 to the one at the time of the last process (Step S14). Then the procedure advances to the step S2 in FIG. 11, the application program 9 carried out the process of this time.

[0256] On this occasion, since a failure occurred when the data file was closed in the last process, it can be assumed that the data file 812, and the start serial number and the restoration data in the recovery information unit 815 have been properly updated in the last process. Therefore, it is possible to execute the process of this time with a proper recovery information unit 25 only if the end serial number is restored to the one at the time of the last process.

[0257] If it is judged in the step S13 that the check serial numbers attached before and after the end serial number is in agreement, the next judgement is made as to whether the start serial number and the end serial number are in agreement or not (Step S15). If in disagreement, it is judged that a failure has occurred during the data file updating operation carried out by the data file updating unit 822 in the last process, then a demand to reprocess the last process and a demand to restore the data in the data file 812 are outputted to the application program 9 and the data restoring unit 831, respectively.

[0258] When receiving a command to restore the data in the data file 812 from the system failure detecting unit 828, the data restoring unit 831 restores the data in the

application area 814 in the data file 812 on the basis of the restoration data stored in the recovery information unit 815 (Step S16). The procedure then advances to the step S2 in FIG. 11, where the application program 9 carries out once more the operation that should have been done in the last process.

[0259] On this occasion, since a failure has occurred during the updating process in the last process, the application area 814 in the data file 812 is restored to the state at the time of two updating processes earlier (the state before the failure has occurred), then a reprocess is demanded to the application program 9, thereby re-executing the last process on the data file 22 that is in a state at the time of two updating processes earlier.

[0260] When the data restoring unit 831 restores the data, the restoration data writing unit 833 writes only the restoration data whose check serial numbers attached before and after the same have been judged by the restoration data effectiveness detecting unit 832 to be in agreement into the data file 812.

[0261] It is therefore possible to restore the data without using the restoration data (whose check serial numbers are in disagreement) that a system failure has occurred in the course of writing the same in the last process.

[0262] In the case where the start serial number is in agreement with the end serial number in the step S15, it is judged to be normal (Step S17), the procedure advances to the step S2 in FIG. 11, where the process of this time is executed by the application program 9.

[0263] Next, operation of the IC card according to this embodiment will be described referring to FIGS. 13 through 16, where a content of practical data in the recovery information unit 815 is shown to explain the operation.

[0264] The recovery information unit 815 immediately after the issue of the IC card 8 is in a state where the start serial number, the end serial number and the restoration data are all set at 0, and the check serial numbers attached before and after the start serial number, the end serial number and the restoration data are all set at 1, as shown in FIG. 13A.

[0265] Assuming that a WRITE instruction for, for example, the record numbers #10, #8 and #11 of the data file 812 from the application program 9 is successively executed between an open and close of the data file 812 without a break due to a system failure, in the first updating process done on the IC card 8.

[0266] In which case, the start serial number obtaining unit 821 and the end serial number obtaining unit 823 obtain "1" and "1" as a start serial number and an end serial number, respectively, to write them into the recovery information unit 815. At the same time, the restoration data obtaining unit 825 also obtains, for example, "#10,3030", "#08,F1F1" and "#11,1010" as restoration data, and writes them into the recovery information unit 815. Before and after each data, check serial numbers "2" are attached, as shown in FIG. 13B.

[0267] Here, "3030", "F1F1" and "1010" in the restoration data are unupdated data at the record numbers #10, #08 and #11 in the application area 814.

[0268] Thereafter, the restoration data initializing unit 827 initializes to make all the restoration data to be "0" and their check serial numbers to be "1" when the second updating process is performed on the IC card 8. Assuming that after the initialization has been executed by the restoration data initializing unit 827, a WRITE instruction is successively executed two times on the record number #02 of the data file 812, and this updating process is executed between an open and close of the data file 812, without a break due to a system failure.

[0269] In which case, the start serial number obtaining unit 821 and the end serial number obtaining unit 823 obtain "2" and "2" as a start serial number and an end serial number, respectively, and write them into the recovery information unit 815. At the same time, the restoration data obtaining unit 825 obtains, for example "02,4040" as restoration data, and also writes it into the recovery information unit. Check serial numbers "3" are attached before and after the start serial number, the end serial number and the restoration data, and also written into the recovery information unit 815.

[0270] In the case where updating process is executed a plurality of times on the same record number in the between an open and close of the data file 812, the restoration data obtaining unit 825 does not write the restoration data into the recovery information unit 815 after the second process and later. "4040" written as unupdated data of the restoration data is the first unupdated data in relation to the record number #02" in the application area 814.

[0271] On the third updating process done on the IC card 8, the restoration data initializing unit 827 first executes initialization. The application program 9 next gives a WRITE instruction for, for example, the record number #10 and #08 in the data file 812. Now assuming that a system failure occurred after restoration data in connection with the record number #08 was obtained, as shown in FIG. 14.

[0272] In which case, the start serial number obtaining unit 821 obtains a start serial number "3" and its check serial numbers "4", and writes them into the recovery information unit 815. The end serial number obtaining unit 823, however, cannot obtain an end serial number and its check serial numbers since a system failure has occurred before receiving a CLOSE instruction. As a result, the end serial number "2" and the check serial number "3" at the time of the last process remain in the recovery information unit 815.

[0273] The restoration data obtaining unit 825 obtains, for example, "#10,3030" and "#08,F1F1" as restoration data, and successively writes them with their check serial numbers "4" into the recovery information unit. The updating process is terminated.

[0274] If the application program 9 executes an updating process on the IC card 8 under the above condi-

tion, the system failure detecting unit 828 operates in response to an OPEN instruction from the application program 9, and makes a judgement that a system failure has occurred during the last updating process since the check serial number attached before and after the start serial number and the check serial numbers attached before and after the end serial number are individually in agreement but the start serial number and the end serial number are in disagreement (referring to Step S15 in FIG. 12). The system failure detecting unit 828 thus outputs a demand to perform a reprocess to the application program 9 and a demand to restore the data in the data file 812 to the data restoring unit 831 (referring to the Step 16 in FIG. 12).

[0275] When the data restoring unit 831 restores the data, the restoration data effectiveness detecting unit 832 verifies the effectiveness of restoration data from whether check serial numbers attached before and after the restoration data are in agreement or not. In the example shown in FIG. 14, the check serial numbers attached before and after two restoration data are all "4", being thus in agreement. The two restoration data are thus judged to be effective. The restoration data writing unit 833 writes the restoration data "3030" and "F1F1" into the respective record numbers #10 and #08 in the application area 814 in the data file 812 on the basis of the above two restoration data whose effectiveness has been verified.

[0276] On the contrary, assuming that upon performing the third updating process on the IC card 8, a WRITE instruction from the application program 9 is executed on the record numbers, for example, #03 and #02 in the data file 812, and a system failure occurs while the restoration data in connection to the record number #2 is being obtained, as shown in FIG. 15.

[0277] In which case, the start serial number obtaining unit 821 obtains a start serial number "3" and its check serial numbers "4", and write them into the recovery information unit 815. The end serial number obtaining unit 823, however, cannot obtain an end serial number and its check serial numbers since a system failure has occurred before receiving a CLOSE instruction. As a result, the end serial number "2" and the check serial number "3" at the time of the last process remain in the recovery information unit 815.

[0278] The restoration data obtaining unit 825 obtains "#03,3232" as restoration data and its check serial numbers "4". However, since a system failure has occurred in the course of obtaining "#02,2222" as the second restoration data, check serial numbers "4" are attached before the restoration data "#02,2222" while check serial numbers "3" attached after the restoration data in the last process still remains even at the end of the process.

[0279] Under such condition, if an updating process is executed on the IC card 8 from the application program 9, the system failure detecting unit 828 operates in response to an OPEN instruction from the application program 9, and makes a judgement that a system failure

has occurred during the last updating process since a check serial number attached before and after the start serial number and a check serial number attached before and after the end serial number are individually in agreement, but the start serial number and the end serial number are in disagreement (referring to the step 15 in FIG. 12). The system failure detecting unit 828 thus outputs a demand to once more perform the last process to the application program 9 besides a demand to restore the data in the data file 812 to the data restoring unit 831, as same as in the example shown in FIG. 14 (referring to the Step S16 in FIG. 12).

[0280] Here, when the data restoring unit 831 restores the data, the restoration data effectiveness detecting unit 832 verifies the effectiveness of the restoration data by making a judgement as to whether the check serial numbers attached before and after the restoration data are in agreement or not. In the example shown in FIG. 15, the check serial numbers attached before and after the first restoration data are both "4", being thus in agreement. But, the check serial numbers attached before and after the second restoration data are "4" and "3", being thus in disagreement.

[0281] For this, the first restoration data is judged to be effective, but it is judged that a system failure has occurred in the course of obtaining the second restoration data so that the updating process on the record number #02 in the application area 814 has not been completed. Therefore, the restoration data writing unit 833 conducts the writing on the basis only the first restoration data.

[0282] Through the above process, it is possible to restore the application area 814 to a state before a system failure has occurred from a state of the system failure as shown in FIG. 16B, by writing the restoration data "3232" to the record number #3 in the application area 814 of the data file 812, respectively.

[0283] As above, a start serial number and an end serial number in the recovery information unit 815 are compared with each other. If the start serial number and the end serial number are in disagreement, it is possible to detect that a system failure has occurred in the course from an open to close of the data file 812. Check serial numbers attached before and after each data in the recovery information unit 815 are also compared with each other. If the check serial numbers are in disagreement, it is possible to detect that a system failure occurred in the course of writing the start serial number, the restoration data or the end serial number into the recovery information unit 815, further detect effectiveness of each data stored in the recovery information unit 815 and conflicting data generated due to the system failure without using a BCC, with certainty.

[0284] Before the restoration data has been obtained by the restoration data obtaining unit 825 is written into the recovery information unit 815, the restoration data of the last process stored in the recovery information unit 815 is initialized by the restoration data initializing unit

827. This initializing operation can prevent the restoration data of the last process from remaining in the recovery information unit when the new restoration data is written in the recovery information unit, and also can surely avoid to erroneously detect a system failure.

[0285] In the case where the data file updating unit 822 executes updating process more than once on the same record number between an open and close of the data file 812, the restoration data obtaining unit 825 does not write the restoration data in the recovery information unit 815 after the second updating and later, whereby it is possible to always hold the data before the data file is opened (i.e., the data before the updating) as the restoration data in the recovery information unit 815 at the same record number. Therefore, the state within the IC card 8 after the system failure has occurred can be effectively restored to the state before the system failure has occurred, on the basis of the data in the recovery information unit 815.

[0286] Since information about the presence of the recovery information unit 815 and information about a relative position of the recovery information unit 815 in a data file if the recovery information unit 815 exists in the data file are both set in the directory area 813 in the storage unit 81, it is possible to make a judgement as to whether predetermined data should be written into the recovery information unit 815 or data should be restored on the basis of the data stored in the recovery information unit, only by referring to the directory area 813 in the storage unit 81 from the control unit 82.

[0287] If the data file 812 has the recovery information unit therein, the system failure detecting unit 828 detects a system failure that has occurred in the last process, on the basis of the start serial number, the end serial number and the check serial numbers attached before and after the start serial number and the end serial number in the recovery information unit 815, in response to an OPEN instruction from the application program 9. This enables an automatic detection of conflicting data occurring due to a system failure within the IC card 8 without using a BCC.

[0288] According to a result of detection carried out by the system failure detecting unit 828, the start serial number restoring unit 829, the end serial number restoring unit 830 and the data restoring unit 831 can automatically repair and restore the recovery information unit 815 or the application area 814, whereby a configuration of the system can be simplified and inconvenience to the owner upon restoring the data can be mitigated to a considerable degree.

[0289] When the data restoring unit 813 repairs the data, the restoration data writing unit 833 writes only the effective restoration data whose check serial numbers attached before and after the same have been judged to be in agreement by the restoration data effectiveness judging unit 832 into the application area 814 in the data file 812. In consequence, it is possible to restore, certainly and effectively, the data in the application area 814

to the state before a system failure has occurred, without using restoration data that the system failure has occurred in the course of the writing (i.e., data whose check serial numbers are in disagreement).

[0290] In the IC card 8, a terminal used to send and receive information to and from the outside (a contact and a data communication mechanism) is omitted in the drawings.

[0291] In the second embodiment state above, there is no need to add the recovery information unit 815 to all data file 812. As shown in FIG. 9, it is possible to omit the recovery information unit 815 in the data file 812 that needs no data recovery.

[0292] In the second embodiment, description has been made by way of an IC card as a card type storage medium. This invention is, however, not limited to the above examples, but adaptable to another type of card type storage medium, for example, an optical card, bringing the same effect as the above examples.

[0293] It is also possible to form a card type storage medium having a function of the IC card 6 according to the invention as claimed, along with a function of the IC card 8 according to the embodiment disclosed in FIGS. 8 - 16. In this case, the advantages of the above two embodiments can be realized in one card type storage medium.

Claims

1. A card type storage medium comprising a storage unit having a file area (21) holding data in each file as a unit and a directory area (23) holding therein control information units (231) each including a PIN of a data file in said file area and a control unit (3) managing data files (22) in said file area (21) in said storage unit (2) on the basis of said control information units (231) in said directory area (23) in said storage unit (2), said control unit (3) allowing an access process on a data file (22) by said control unit (3) only when a PIN held in said control information unit (231) in said directory area (23) in said storage unit (2) is in agreement with a PIN inputted from outside, the storage medium further comprising:
 - a dedicated file (24) being set in said file area (21) in said storage unit (2), said dedicated file (24) holding PINs of the data files (22) held in said respective control information units (231) in said directory area (23) in said storage unit (2) and file names of the data file (22) such that the PIN and the file name of each data file (22) correspond to each other;
 - another control information unit (232) being set in said directory area (23) in said storage unit (2), said control information unit (232) holding a master PIN of said dedicated file (24).
2. A card type storage medium according to claim 1, wherein the PINs of the respective data files (22) are enciphered to be held in said dedicated file (24).
3. A card type storage medium comprising:
 - a storage unit (2) having a file area (21) for holding data in each file as a unit and a directory area (23) for holding therein control information units (231) each including a PIN of each data file (22) in said file area (21);
 - a control unit (3) managing data files (22) in said file area (21) in said storage unit (2) on the basis of said control information units (231) in said directory area (23) in said storage unit (2), said control unit (3) comprising:
 - a data file creating means (31), in response to a data file creating command from outside, setting a control information unit (231) for a data file (22) including a PIN of said data file (22) to create said data file (22) in said file area (21) in said storage unit (2) according to said data file creating command;
 - a PIN matching means (32), in response to a data file access command to gain an access to the data file (22) created by said data file creating means (31) from the outside, making a judgement as to whether the PIN of said data file (22) to be accessed according to said data file access command held in said control information unit (231) in said directory area (23) in said storage unit (2) is in agreement with a PIN included in said data file access command supplied from the outside;
 - a data file accessing means (32) executing an access process on the data file (22) to be accessed when said PIN matching means (32) judges that said two PINs are in agreement;
 - a dedicated file creating means (34), in response to a dedicated file creating command from the outside, setting a control information unit (232) for said dedicated file (24) including a master PIN for said dedicated file (24) to create said dedicated file (24) in said file area (21) in said storage unit (2) according to said dedicated file creating command;
 - a master PIN matching means (35), in response to a dedicated file access command to gain an access to said dedicated file (24) created by said dedicated file creating means from the outside, making a judgement as to whether the master PIN of said dedicated file (24) held in said control

information unit (232) in said directory area (23) in said storage unit (2) is in agreement with a master PIN included in said dedicated file access command supplied from the outside; and

a dedicated file access means (36) executing an access process on said dedicated file (24) when said master PIN matching means (35) makes a judgement that the above two master PINs are in agreement; upon issuing said IC card, said dedicated file accessing means (36) writing the PINs of the data files (22) held in said respective control information units (231) in said directory area (23) in said storage unit (2) into said dedicated file (24) such that the PIN and file name of each data file (22) correspond to each other according to a dedicated file accessing command supplied from outside after said dedicated file creating means (34) created said dedicated file.

4. A card type storage medium according to claim 3, wherein PINs for the respective data files (22) are enciphered and held in said dedicated file (24).

5. A card type storage medium issuing apparatus issuing a card type storage medium (10), said card type storage medium (10) comprising a storage unit (2) having a file area (21) for holding data in each file as a unit and a directory area (23) for holding therein control information units (231) each including a PIN of a data file (22) in said file area (21) and a control unit (3) managing data files (22) in said file area (21) in said storage unit (2) comprising:

a data file creation instructing means (41) setting a control information unit (231) for a data file (22) including a PIN of the data file (22) in said directory area (23) in said storage unit (2), generating a data file creating command including the PIN of the data file (22), and transferring it to said card type storage medium (10) in order to create the data file (22) in said file area (21) in said storage unit (2);

a data file access instructing means (42) generating a data file accessing command including a PIN of a data file (22) to be accessed, and transferring it to said card type storage medium (10) in order to gain an access to the data file (22) created in the file area (21) in said storage unit (2);

a dedicated file creation instructing means (43) setting a control information unit (232) for a dedicated file (24) including a master PIN of the dedicated file (24) in said directory area (23) in said storage unit (2), generating a dedicated file creating command including the master PIN,

and transferring it to said "card type storage medium (10) in order to create the dedicated file (24) in said file area (21) in said storage unit (2);

a dedicated file access instructing means (44) generating a dedicated file accessing command including the master PIN of the dedicated file (24), and transferring it to said card type storage medium (10) in order to gain an access to the dedicated file (24) created in said file area (21) in said storage unit (2);

upon issuing said card type storage medium (10), after said dedicated file creation instructing means (43) transferred a dedicated file creating command to said card type storage medium (10), said dedicated file access instructing means (44) generating a dedicated file accessing command including data of PINs and file names of the data files (22), and transfers it to said card type storage medium (10), in order to write the PINs and file names of the data files (22) held in said respective control information units (231) in said directory area (23) in said storage unit (2) such that the PIN and file name of each data file (22) correspond to each other.

6. A card type storage medium issuing apparatus according to claim 5, wherein when a PIN of said card type storage medium (10) is verified, said dedicated file access instructing means (44) generates a dedicated file access command including the master PIN, and transfers it to said card type storage medium (10) in order to read out data held in said dedicated file (24) in said file area (22) in said storage unit (2) of said card type storage medium (10) whose PIN is to be verified.

7. A card type storage medium issuing apparatus according to claim 6, wherein when data including a PIN and file name of a data file (22) held in said card type storage medium (10) is read out from said dedicated file (24) of said card type storage medium (10) in response to a dedicated file accessing command send out from said dedicated file access instructing means (44), said data file access instructing means (44) generates a data file accessing command including the PIN read out, and transfers it to said card type storage medium (10) so as to give an instruction to said card type storage medium (10) to verify correctness of the data file (22) corresponding to said PIN read out.

8. A card type storage medium issuing apparatus according to any one of claims 5 through 7, wherein said card type storage medium issuing apparatus further comprises an enciphering means enciphering the PINs of the data files (22) to be written in said dedicated file (24) in said card type storage me-

dium (10) by said dedicated file access instructing means (44), and a deciphering means deciphering an enciphered PIN of a data file (22) read out from said dedicated file (24) in said card type storage medium (10) by said dedicated file access instructing means (44). 5

Patentansprüche

1. Speichermedium des Kartentyps mit einer Speichereinheit, die einen Dateibereich (21) hat, der Daten in jeder Datei als Einheit hält, und einen Verzeichnissbereich (23), in dem Steuerinformationseinheiten (231) gehalten werden, die jeweils eine PIN einer Datendatei in dem Dateibereich enthalten, und einer Steuereinheit (3), die Datendateien (22) in dem Dateibereich (21) in der Speichereinheit (2) auf der Basis der Steuerinformationseinheiten (231) in dem Verzeichnissbereich (23) in der Speichereinheit (2) verwaltet, welche Steuereinheit (3) einen Zugriffsprozeß an einer Datendatei (22) durch die Steuereinheit (3) nur dann gestattet, wenn eine PIN, die in der Steuerinformationseinheit (231) in dem Verzeichnissbereich (23) in der Speichereinheit (2) gehalten wird, mit einer von außen eingegebenen PIN übereinstimmt, welches Speichermedium ferner umfaßt:
 - eine Spezialdatei (24), die in dem Dateibereich (21) in der Speichereinheit (2) festgelegt ist, welche Spezialdatei (24) PINs der Datendateien (22) hält, die in den jeweiligen Steuerinformationseinheiten (231) in dem Verzeichnissbereich (23) in der Speichereinheit (2) gehalten werden, und Dateinamen der Datendatei (22), so daß die PIN und der Dateiname von jeder Datendatei (22) einander entsprechen;
 - eine andere Steuerinformationseinheit (232), die in dem Verzeichnissbereich (23) in der Speichereinheit (2) festgelegt ist, welche Steuerinformationseinheit (232) eine Master-PIN der Spezialdatei (24) hält.
2. Speichermedium des Kartentyps nach Anspruch 1, bei dem die PINs der jeweiligen Datendateien (22) chiffriert sind, um in der Spezialdatei (24) gehalten zu werden.
3. Speichermedium des Kartentyps mit:
 - einer Speichereinheit (2), die einen Dateibereich (21) zum Halten von Daten in jeder Datei als Einheit hat, und einen Verzeichnissbereich (23) zum Halten von Steuerinformationseinheiten (231), die jeweils eine PIN von jeder Datendatei (22) in dem Dateibereich (21) enthalten;
 - einer Steuereinheit (3), die Datendateien (22)

in dem Dateibereich (21) in der Speichereinheit (2) auf der Basis der Steuerinformationseinheiten (231) in dem Verzeichnissbereich (23) in der Speichereinheit (2) verwaltet, welche Steuereinheit (3) umfaßt:

ein Datendateibildungsmittel (31), das als Antwort auf einen Datendateibildungsbefehl von außen eine Steuerinformationseinheit (231) für eine Datendatei (22) festlegt, die eine PIN der Datendatei (22) enthält, um die Datendatei (22) in dem Dateibereich (21) in der Speichereinheit (2) gemäß dem Datendateibildungsbefehl zu bilden;

ein PIN-Gleichheitsprüfungsmittel (32), das als Antwort auf einen Datendateizugriffsbefehl von außen, um einen Zugriff auf die Datendatei (22) zu erlangen, die durch das Datendateibildungsmittel (31) gebildet wurde, ein Urteil diesbezüglich trifft, ob die PIN der Datendatei (22), auf die gemäß dem Datendateizugriffsbefehl zuzugreifen ist, die in der Steuerinformationseinheit (231) in dem Verzeichnissbereich (23) in der Speichereinheit (2) gehalten wird, mit einer PIN übereinstimmt, die in dem Datendateizugriffsbefehl enthalten ist, der von außen zugeführt wurde;

ein Datendateizugriffsmittel (32), das einen Zugriffsprozeß an der Datendatei (22) ausführt, auf die zuzugreifen ist, wenn das PIN-Gleichheitsprüfungsmittel (32) beurteilt, daß die zwei PINs übereinstimmen;

ein Spezialdateibildungsmittel (34), das als Antwort auf einen Spezialdateibildungsbefehl von außen eine Steuerinformationseinheit (232) für die Spezialdatei (24) festlegt, die eine Master-PIN für die Spezialdatei (24) enthält, um die Spezialdatei (24) in dem Dateibereich (21) in der Speichereinheit (2) gemäß dem Spezialdateibildungsbefehl zu bilden;

ein Master-PIN-Gleichheitsprüfungsmittel (35), das als Antwort auf einen Spezialdateizugriffsbefehl von außen, um einen Zugriff auf die Spezialdatei (24) zu erlangen, die durch das Spezialdateibildungsmittel gebildet wurde, ein Urteil diesbezüglich trifft, ob die Master-PIN der Spezialdatei (24), die in der Steuerinformationseinheit (232) in dem Verzeichnissbereich (23) in der Speichereinheit (2) gehalten wird, mit einer Master-PIN übereinstimmt, die in dem Spezialdateizugriffsbefehl enthalten ist, der von außen zugeführt wurde; und

ein Spezialdateizugriffsmittel (36), das einen Zugriffsprozeß an der Spezialdatei

(24) ausführt, wenn das Master-PIN-Gleichheitsprüfungsmittel (35) das Urteil trifft, daß die obigen zwei Master-PINs übereinstimmen;

5

wobei das Spezialdateizugriffsmittel (36), bei der Ausgabe der IC-Karte, die PINs der Datendateien (22), die in den jeweiligen Steuerinformationseinheiten (231) in dem Verzeichnisbereich (23) in der Speichereinheit (2) gehalten werden, in die Spezialdatei (24) schreibt, so daß die PIN und der Dateiname von jeder Datendatei (22) einander entsprechen, gemäß einem Spezialdateizugriffsbefehl, der von außen zugeführt wird, nachdem das Spezialdateibildungsmittel (34) die Spezialdatei bildet.

10

15

4. Speichermedium des Kartentyps nach Anspruch 3, bei dem PINs für die jeweiligen Datendateien (22) chiffriert sind und in der Spezialdatei (24) gehalten werden.

20

5. Ausgabevorrichtung von Speichermedien des Kartentyps, die ein Speichermedium des Kartentyps (10) ausgibt, welches Speichermedium des Kartentyps (10) eine Speichereinheit (2) umfaßt, die einen Dateibereich (21) zum Halten von Daten in jeder Datei als Einheit hat, und einen Verzeichnisbereich (23), zum Halten von Steuerinformationseinheiten (231), die jeweils eine PIN einer Datendatei (22) in dem Dateibereich (21) enthalten, und eine Steuerinformationseinheit (3), die Datendateien (22) in dem Dateibereich (21) in der Speichereinheit (2) verwaltet, mit:

25

30

einem Datendateibildungsinstruktionsmittel (41), das eine Steuerinformationseinheit (231) für eine Datendatei (22), die eine PIN der Datendatei (22) enthält, in dem Verzeichnisbereich (23) in der Speichereinheit (2) festlegt, einen Datendateibildungsbefehl erzeugt, der die PIN der Datendatei (22) enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um die Datendatei (22) in dem Dateibereich (21) in der Speichereinheit (2) zu bilden; einem Datendateizugriffsinstruktionsmittel (42), das einen Datendateizugriffsbefehl erzeugt, der eine PIN einer Datendatei (22) enthält, auf die zuzugreifen ist, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um einen Zugriff auf die Datendatei (22) zu erlangen, die in dem Dateibereich (21) in der Speichereinheit (2) gebildet wurde; einem Spezialdateibildungsinstruktionsmittel (43), das eine Steuerinformationseinheit (232) für eine Spezialdatei (24), die eine Master-PIN der Spezialdatei (24) enthält, in dem Verzeichnisbereich (23) in der Speichereinheit (2) festlegt, einen Spezialdateibildungsbefehl erzeugt,

35

40

45

50

55

der die Master-PIN enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um die Spezialdatei (24) in dem Dateibereich (21) in der Speichereinheit (2) zu bilden; einem Spezialdateizugriffsinstruktionsmittel (44), das einen Spezialdateizugriffsbefehl erzeugt, der die Master-PIN der Spezialdatei (24) enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um einen Zugriff auf die Spezialdatei (24) zu erlangen, die in dem Dateibereich (21) in der Speichereinheit (2) gebildet wurde;

welches Spezialdateizugriffsinstruktionsmittel (44), bei der Ausgabe des Speichermediums des Kartentyps (10), nachdem das Spezialdateibildungsinstruktionsmittel (43) einen Spezialdateibildungsbefehl zu dem Speichermedium des Kartentyps (10) übertrug, einen Spezialdateizugriffsbefehl erzeugt, der Daten von PINs und Dateinamen der Datendateien (22) enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um die PINs und Dateinamen der Datendateien (22), die in den jeweiligen Steuerinformationseinheiten (231) in dem Verzeichnisbereich (23) in der Speichereinheit (2) gehalten werden, zu schreiben, so daß die PIN und der Dateiname von jeder Datendatei (22) einander entsprechen.

6. Ausgabevorrichtung von Speichermedien des Kartentyps nach Anspruch 5, bei der das Spezialdateizugriffsinstruktionsmittel (44), wenn eine PIN des Speichermediums des Kartentyps (10) verifiziert wird, einen Spezialdateizugriffsbefehl erzeugt, der die Master-PIN enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um Daten auszulesen, die in der Spezialdatei (24) in dem Dateibereich (22) in der Speichereinheit (2) des Speichermediums des Kartentyps (10) gehalten werden, dessen PIN zu verifizieren ist.

7. Ausgabevorrichtung von Speichermedien des Kartentyps nach Anspruch 6, bei der das Datendateizugriffsinstruktionsmittel (42), wenn Daten, die eine PIN und einen Dateinamen einer Datendatei (22) enthalten, die in dem Speichermedium des Kartentyps (10) gehalten wird, aus der Spezialdatei (24) des Speichermediums des Kartentyps (10) als Antwort auf einen Spezialdateizugriffsbefehl ausgelesen werden, der von dem Spezialdateizugriffsinstruktionsmittel (44) ausgesendet wurde, einen Datendateizugriffsbefehl erzeugt, der die ausgelesene PIN enthält, und ihn zu dem Speichermedium des Kartentyps (10) überträgt, um dem Speichermedium des Kartentyps (10) eine Instruktion zum Verifizieren der Korrektheit der Datendatei (22) zu erteilen, die der ausgelesenen PIN entspricht.

8. Ausgabevorrichtung von Speichermedien des Kartentyps nach irgendeinem der Ansprüche 5 bis 7, welche Ausgabevorrichtung von Speichermedien des Kartentyps ferner ein Chiffriermittel umfaßt, das die PINs der Datendateien (22) chiffriert, um in die Spezialdatei (24) in dem Speichermedium des Kartentyps (10) durch das Spezialdateizugriffsinstruktionsmittel (44) geschrieben zu werden, und ein Dechiffriermittel, das eine chiffrierte PIN einer Datendatei (22) dechiffriert, die aus der Spezialdatei (24) in dem Speichermedium des Kartentyps (10) durch das Spezialdateizugriffsinstruktionsmittel (44) ausgelesen wurde.

Revendications

1. Un support de stockage de type carte comprenant une unité de stockage ayant une zone de fichiers (21) conservant des données dans chaque fichier en tant qu'unité, et une zone de répertoire (23) conservant à l'intérieur des unités d'information de commande (231) incluant chacune un numéro d'identification personnel, ou PIN, d'un fichier de données dans la zone de fichiers, et une unité de commande (3) gérant des fichiers de données (22) dans la zone de fichiers (21) de l'unité de stockage (2) sur la base des unités d'information de commande (231) dans la zone de répertoire (23) dans l'unité de stockage (2), l'unité de commande (3) autorisant un processus d'accès sur un fichier de données (22) par l'unité de commande (3) seulement lorsqu'un PIN conservé dans l'unité d'information de commande (231) dans la zone de répertoire (23) dans l'unité de stockage (2) concorde avec un PIN introduit à partir de l'extérieur, le support de stockage comprenant en outre :
- un fichier dédié (24) qui est établi dans la zone de fichiers (21) dans l'unité de stockage (2), ce fichier dédié (24) conservant des PIN des fichiers de données (22) conservés dans les unités de commande d'information (231) respectives dans la zone de répertoire (23) dans l'unité de stockage (2) et des noms de fichier du fichier de données (22), de façon que le PIN et le nom de fichier de chaque fichier de données (22) correspondent l'un à l'autre;
- une autre unité d'information de commande (232) étant établie dans la zone de répertoire (23) dans l'unité de stockage (2), cette unité d'information de commande (232) conservant un PIN maître du fichier dédié (24).
2. Un support de stockage du type carte selon la revendication 1, dans lequel les PIN des fichiers de données (22) respectifs sont chiffrés pour être conservés dans le fichier dédié (24).

3. Un support de stockage de type carte comprenant une unité de stockage (2) ayant une zone de fichiers (21) pour conserver des données dans chaque fichier en tant qu'unité, et une zone de répertoire (23) pour conserver à l'intérieur des unités d'information de commande (231) incluant chacune un numéro d'identification personnel, ou PIN, de chaque fichier de données (22) dans la zone de fichiers (21);

une unité de commande (3) gérant des fichiers de données (22) dans la zone de fichiers (21) dans l'unité de stockage (2), sur la base des unités d'information de commande (231) dans la zone de répertoire (23) dans l'unité de stockage (2), l'unité de commande (3) comprenant :

un moyen de création de fichier de données (31) qui, en réponse à un ordre de création de fichier de données provenant de l'extérieur, fixe une unité d'information de commande (231) pour un fichier de données (22) incluant un PIN du fichier de données (22), pour créer le fichier de données (22) dans la zone de fichiers (21) dans l'unité de stockage (2), conformément à l'ordre de création de fichier de données;

un moyen de comparaison de PIN (32) qui, en réponse à un ordre d'accès de fichier de données pour obtenir un accès au fichier de données (22) créé par le moyen de création de fichier de données (31) à partir de l'extérieur, juge si le PIN du fichier de données (22) sur lequel doit porter l'accès, conformément à l'ordre d'accès de fichier de données conservé dans l'unité d'information de commande (231) dans la zone de répertoire (23) dans l'unité de stockage (2), concorde avec un PIN inclus dans l'ordre d'accès de fichier de données fourni à partir de l'extérieur;

un moyen d'accès de fichier de données (32) exécutant un processus d'accès sur le fichier de données (22) auquel il est nécessaire d'accéder, lorsque le moyen de comparaison de PIN (32) juge que les deux PIN sont en concordance;

un moyen de création de fichier dédié (34) qui, en réponse à un ordre de création de fichier dédié provenant de l'extérieur, fixe une unité d'information de commande (232) pour le fichier dédié (24), incluant un PIN maître pour le fichier dédié (24), pour créer le fichier dédié (24) dans la zone de fichiers (21) dans l'unité de stockage (2), conformément à l'ordre de création de fichier dédié;

un moyen de comparaison de PIN maître (35) qui, en réponse à un ordre d'accès de fichier dédié pour accéder au fichier dédié (24), créé par le moyen de création de fichier dédié, provenant de l'extérieur, juge si le PIN maître du

fichier dédié (24) conservé dans l'unité d'information de commande (232) dans la zone de répertoire (23) dans l'unité de stockage (2), concorde avec un PIN maître inclus dans l'ordre d'accès de fichier dédié fourni à partir de l'extérieur; et
 un moyen d'accès de fichier dédié (36) exécutant un processus d'accès sur le fichier dédié (24) lorsque le moyen de comparaison de PIN maître (35) juge que les deux PIN maîtres ci-dessus concordent;
 au moment de l'émission de la carte à circuit intégré, ou CI, le moyen d'accès de fichier dédié (36) écrit dans le fichier dédié (24) les PIN des fichiers de données (22) conservés dans les unités d'information de commande (231) respectives dans la zone de répertoire (23) dans l'unité de stockage (2), de façon que le PIN et le nom de fichier de chaque fichier de données (22) correspondent l'un à l'autre conformément à un ordre d'accès de fichier dédié fourni à partir de l'extérieur, après que le moyen de création de fichier dédié (34) a créé le fichier dédié.

4. Un support de stockage du type carte selon la revendication 3, dans lequel des PIN pour les fichiers de données (22) respectifs sont chiffrés et conservés dans le fichier dédié (24).

5. Un appareil d'émission de support de stockage du type carte, émettant un support de stockage du type carte (10), ce support de stockage du type carte (10) comprenant une unité de stockage (2) ayant une zone de fichiers (21) pour conserver des données dans chaque fichier en tant qu'unité, et une zone de répertoire (23) pour conserver à l'intérieur des unités d'information de commande (231) incluant chacune un numéro d'identification personnel, PIN, d'un fichier de données (22) dans la zone de fichiers (21), et une unité de commande (3) gérant des fichiers de données (22) dans la zone de fichiers (21) dans l'unité de stockage (2), comprenant :

un moyen de commande de création de fichier de données (41) fixant une unité d'information de commande (231) pour un fichier de données (22) incluant un PIN du fichier de données (22) dans la zone de répertoire (23) dans l'unité de stockage (2), générant un ordre de création de fichier de données incluant le PIN du fichier de données (22), et transférant celui-ci vers le support de stockage du type carte (10) afin de créer le fichier de données (22) dans la zone de fichiers (21) dans l'unité de stockage (2);
 un moyen de commande d'accès de fichier de données (42) générant un ordre d'accès de fi-

chier de données incluant un PIN d'un fichier de données (22) auquel il est nécessaire d'accéder, et transférant celui-ci vers le support de stockage du type carte (10) afin d'obtenir l'accès au fichier de données (22) créé dans la zone de fichiers (21) dans l'unité de stockage (2);
 un moyen de commande de création de fichier dédié (43) fixant une unité d'information de commande (232) pour un fichier dédié (24) incluant un PIN maître du fichier dédié (24) dans la zone de répertoire (23) d'unité de stockage (2), générant un ordre de création de fichier dédié incluant le PIN maître, et transférant celui-ci vers le support de stockage du type carte (10) afin de créer le fichier dédié (24) dans la zone de fichiers (21) dans l'unité de stockage (2);
 un moyen de commande d'accès de fichier dédié (44) générant un ordre d'accès de fichier dédié incluant le PIN maître du fichier dédié (24), et transférant celui-ci vers le support de stockage du type carte (10) afin d'obtenir l'accès au fichier dédié (24) créé dans la zone de fichiers (21) dans l'unité de stockage (2);
 au moment de l'émission du support de stockage du type carte (10), après que le moyen de commande de création de fichier dédié (43) a transféré un ordre de création de fichier dédié vers le support de stockage du type carte (10), le moyen de commande d'accès de fichier dédié (44) générant un ordre d'accès de fichier dédié incluant des données de PIN et des noms de fichiers des fichiers de données (22), et transférant celui-ci vers le support de stockage du type carte (10), afin d'écrire les PIN et les noms de fichiers des fichiers de données (22) conservés dans les unités d'information de commande (231) respectives dans la zone de répertoire (23) dans l'unité de stockage (2), de façon que le PIN et le nom de fichier de chaque fichier de données (22) correspondent l'un à l'autre.

6. Un appareil d'émission de support de stockage du type carte selon la revendication 5, dans lequel lorsqu'un PIN du support de stockage du type carte (10) est vérifié, le moyen de commande d'accès de fichier dédié (44) génère un ordre d'accès de fichier dédié incluant le PIN maître, et transfère celui-ci vers le support de stockage du type carte (10), afin de lire des données conservées dans le fichier dédié (24) dans la zone de fichiers (22) dans la zone de stockage (2) du support de stockage du type carte (10) dont le PIN doit être vérifié.

7. Un appareil d'émission de support de stockage du type carte selon la revendication 6, dans lequel lorsque des données incluant un PIN et un nom de fichier d'un fichier de données (22) conservé dans le

soutien de stockage du type carte (10) sont lues dans le fichier dédié (24) du soutien de stockage du type carte (10), en réponse à un ordre d'accès de fichier dédié émis par le moyen de commande d'accès de fichier dédié (44), le moyen de commande d'accès de fichier dédié (44) génère un ordre d'accès de fichier de données incluant le PIN lu, et le transfère vers le soutien de stockage du type carte (10), de façon à donner une instruction au soutien de stockage du type carte (10) pour vérifier que le fichier de données (22) correspondant au PIN lu est correct.

8. Un appareil d'émission de soutien de stockage du type carte selon l'une quelconque des revendications 5 à 7, dans lequel l'appareil d'émission de soutien de stockage du type carte comprend en outre un moyen de chiffrement qui chiffre les PIN des fichiers de données (22) à écrire dans le fichier dédié (24) dans le soutien de stockage du type carte (10), par le moyen de commande d'accès de fichier dédié (44), et un moyen de déchiffrement qui déchiffre un PIN chiffré d'un fichier de données (22) lu dans le fichier dédié (24) sur le soutien de stockage du type carte (10), par le moyen de commande d'accès de fichier dédié (44).

30

35

40

45

50

55

FIG. 1

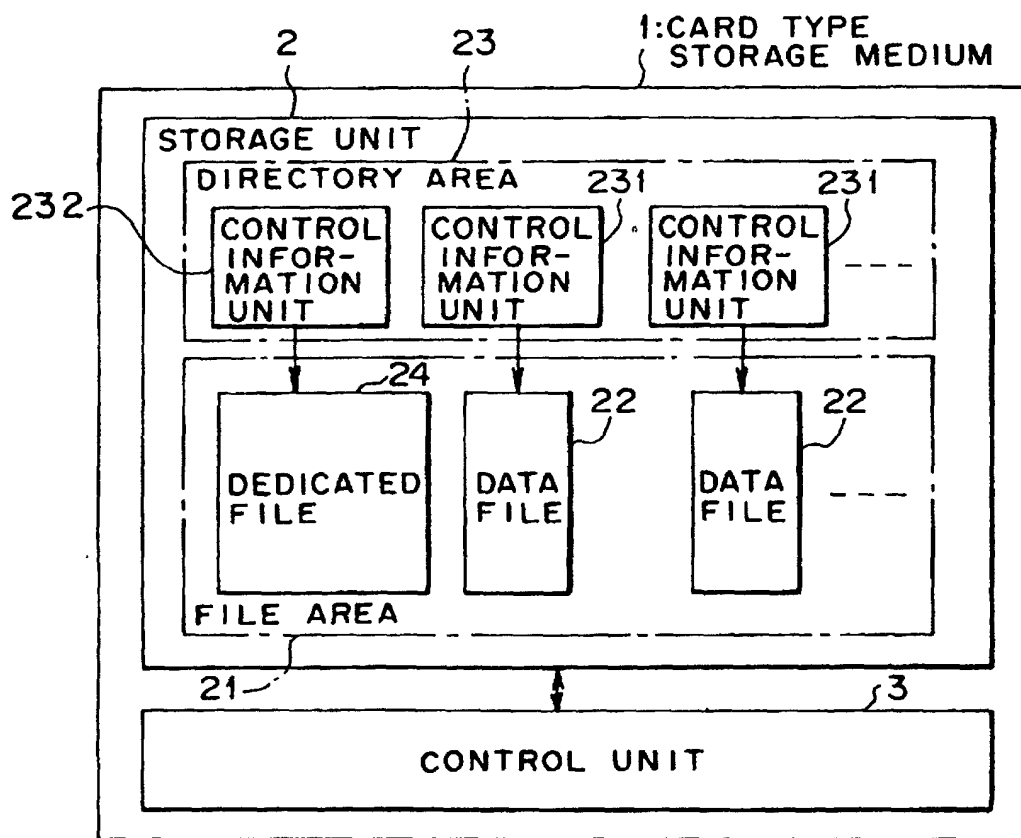


FIG. 2

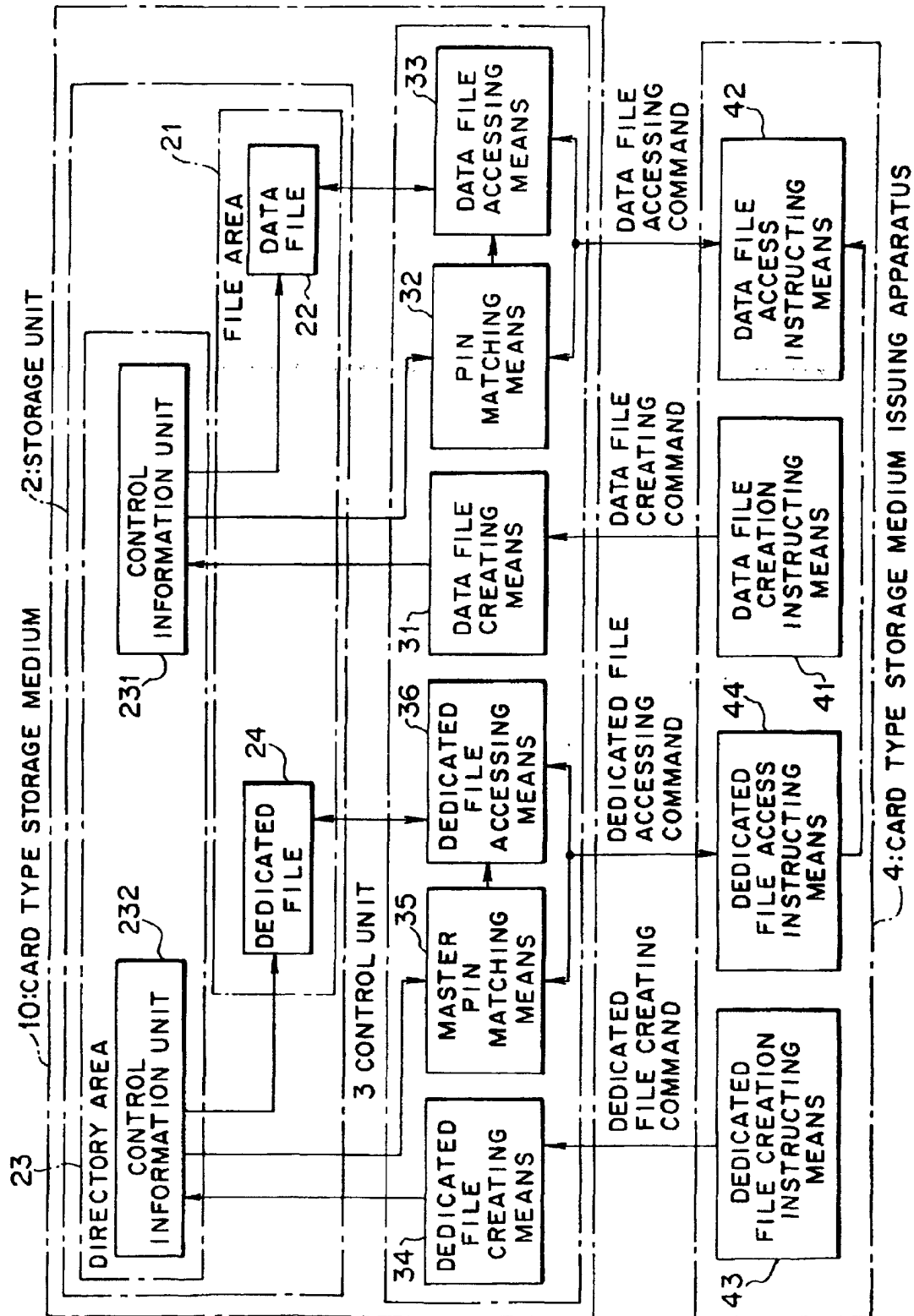


FIG. 3

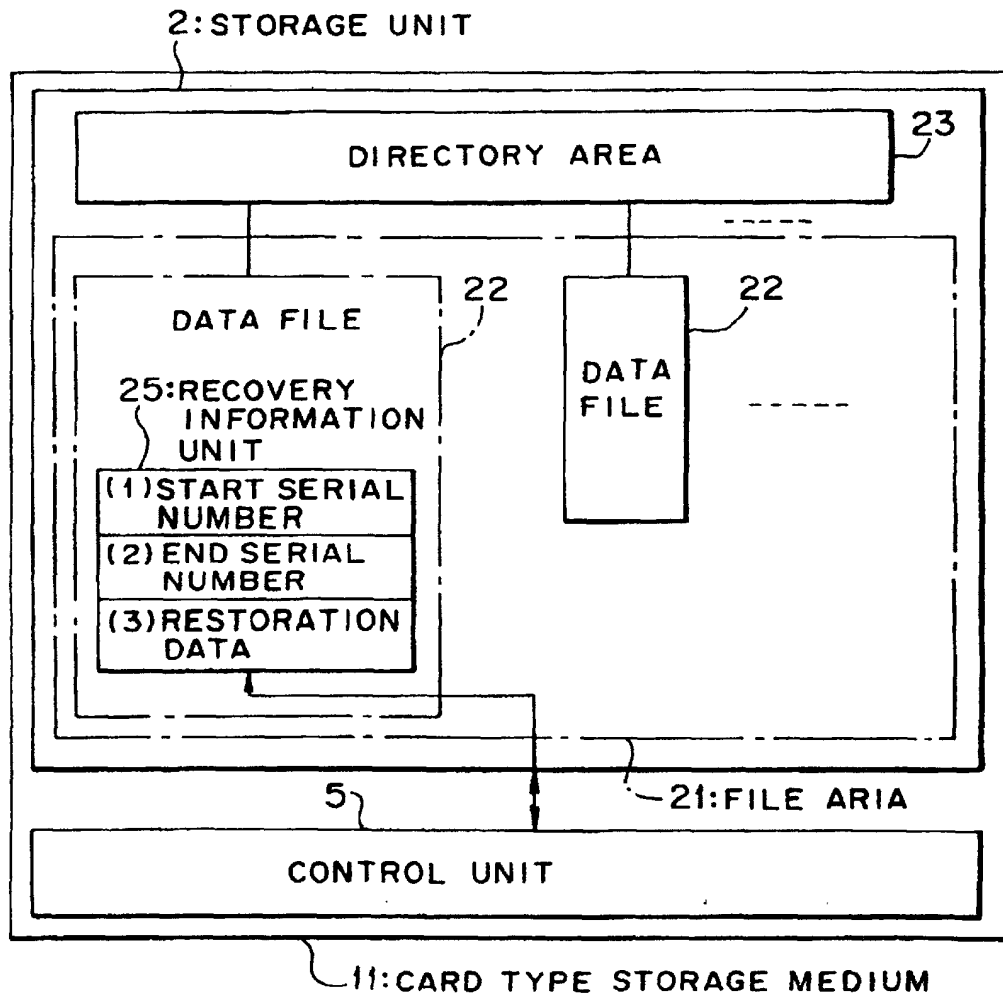


FIG. 4

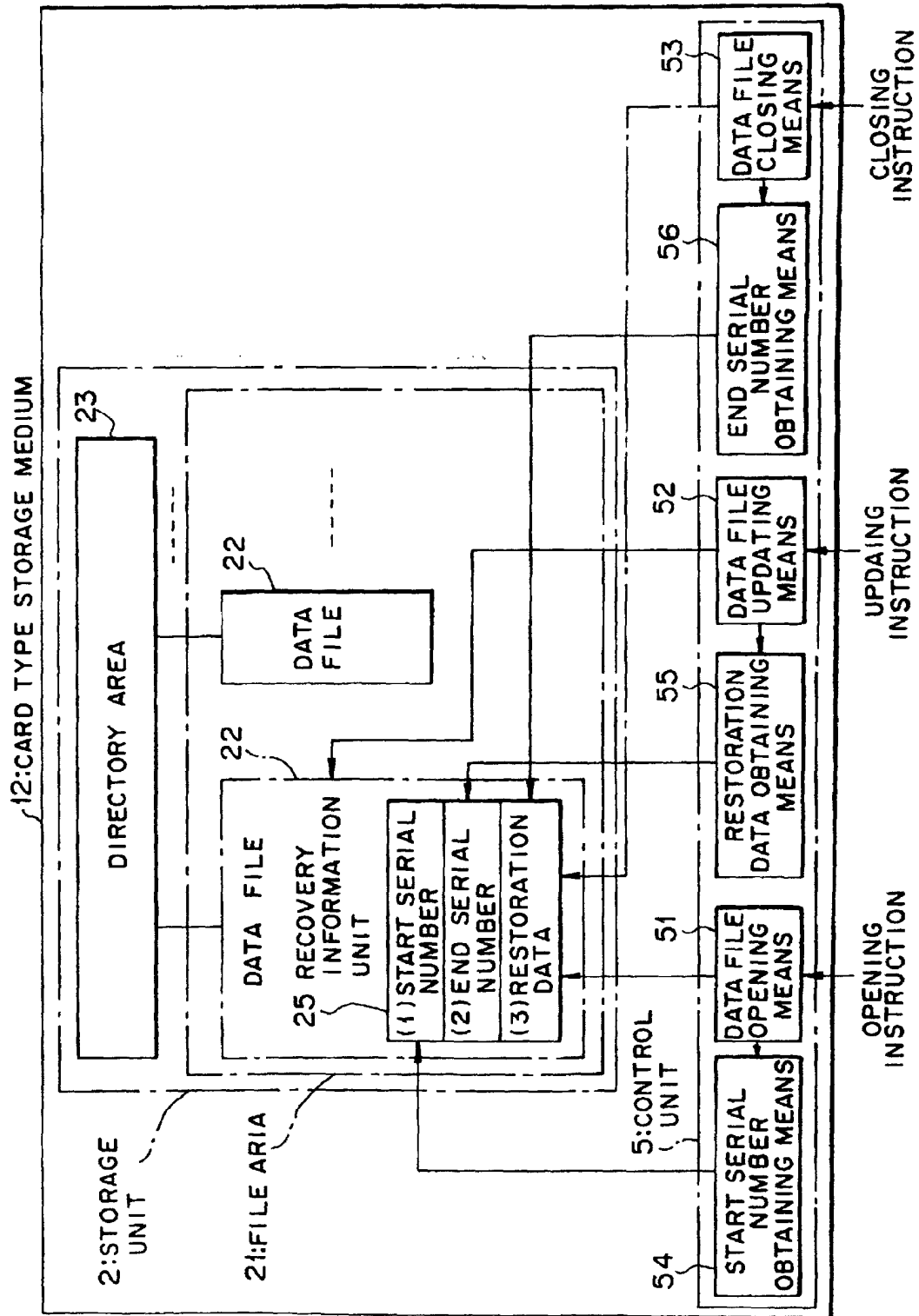


FIG. 5

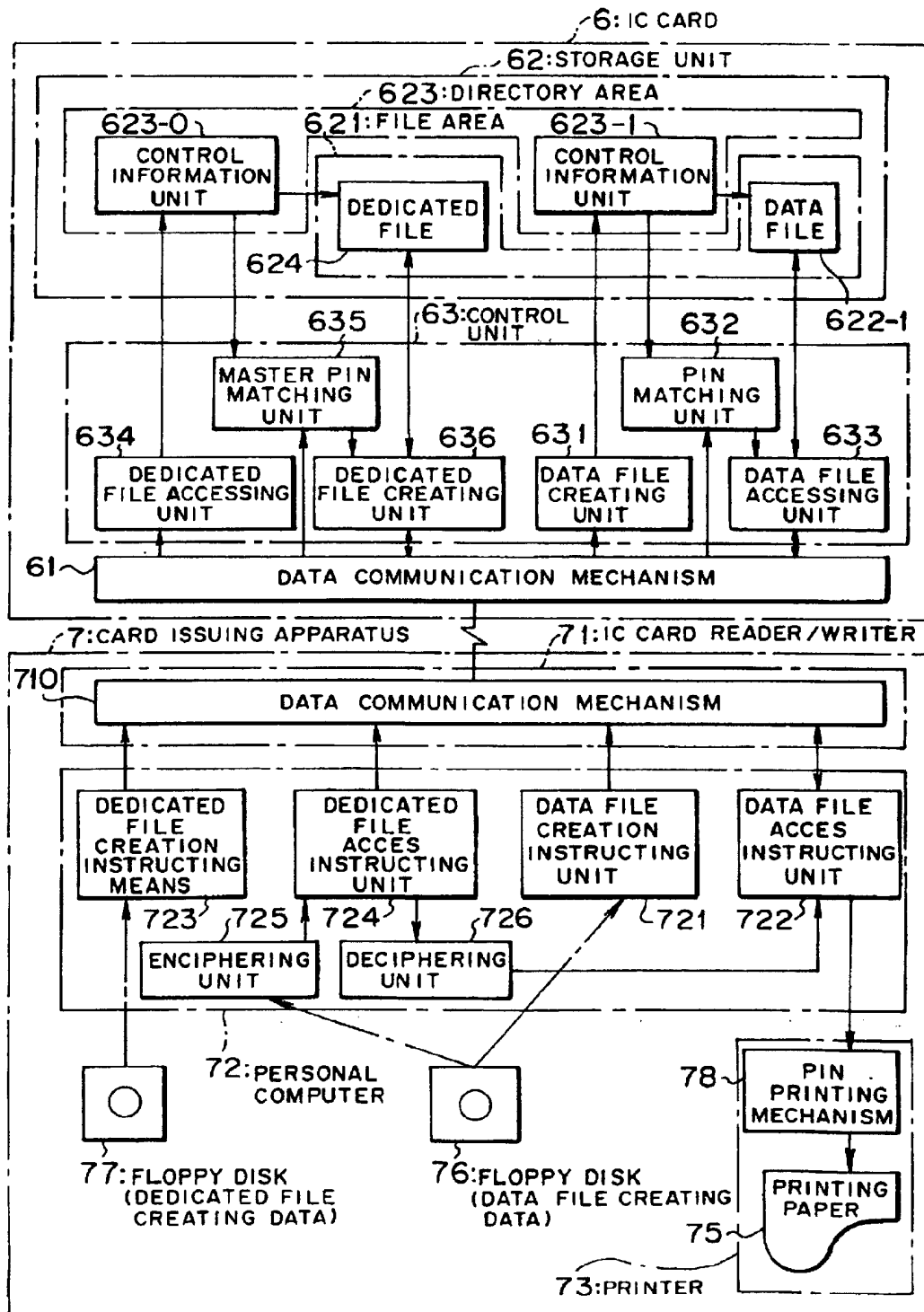


FIG. 6

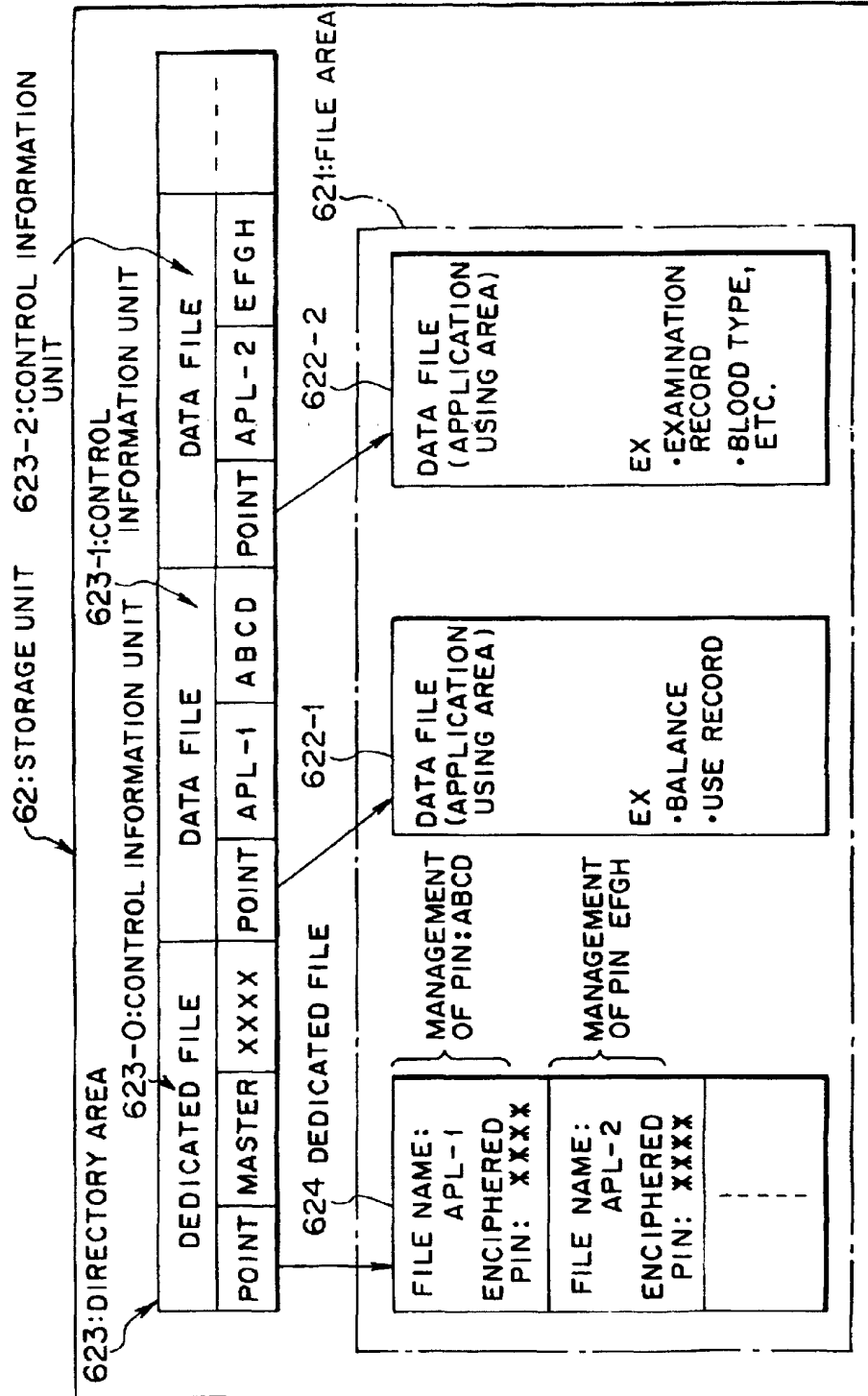


FIG. 7

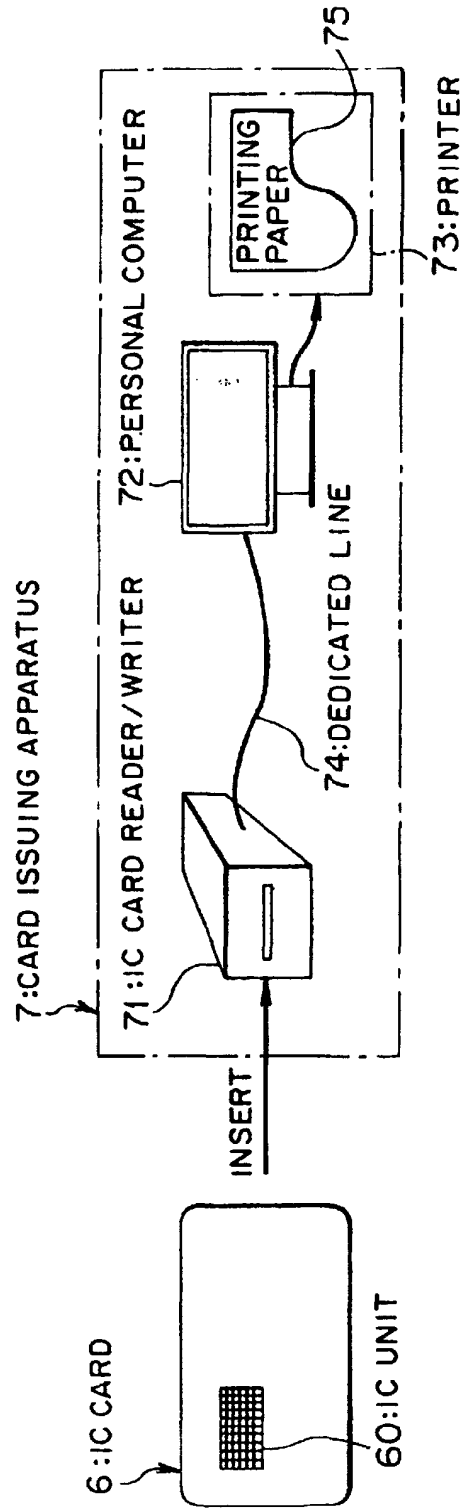


FIG. 8

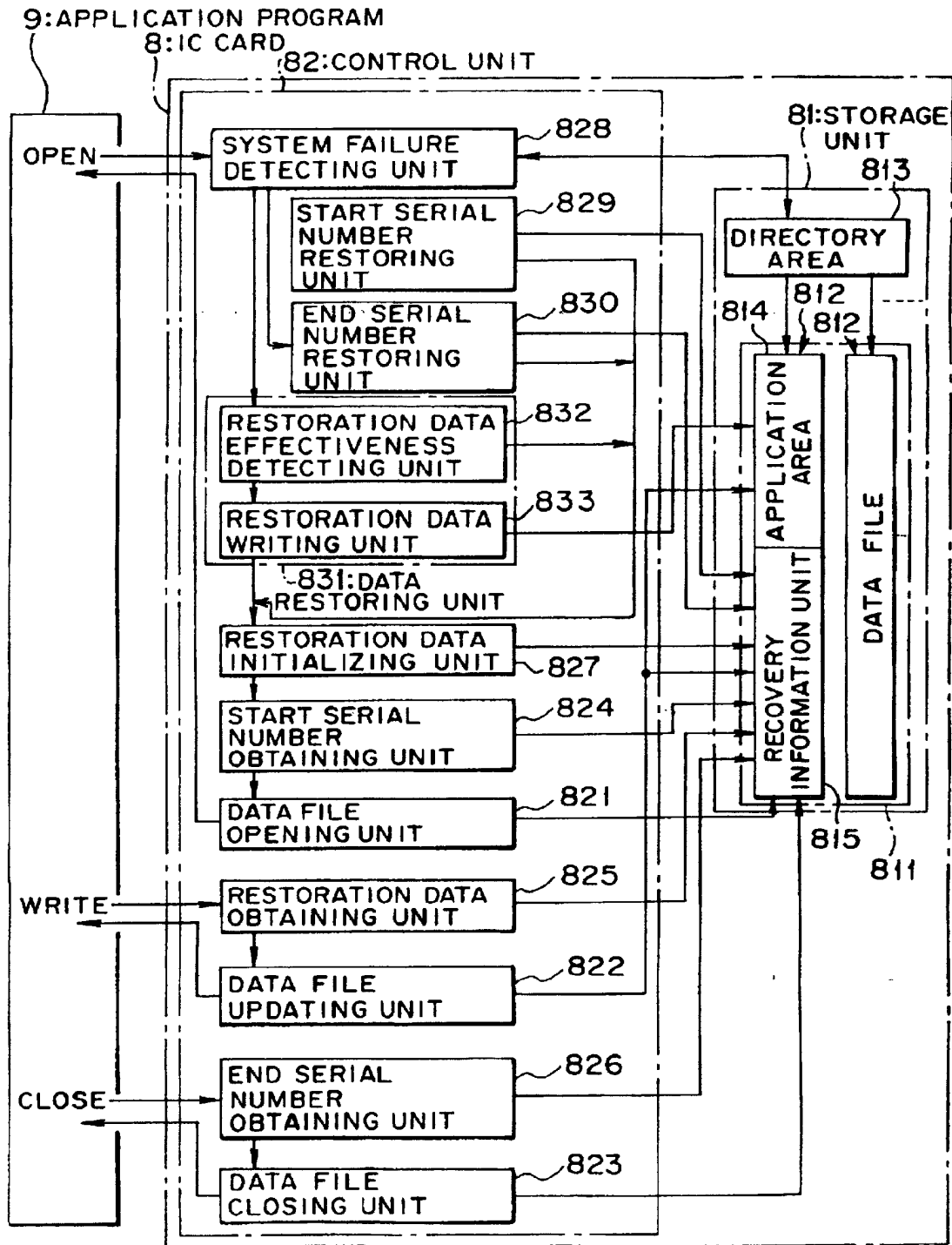


FIG. 9

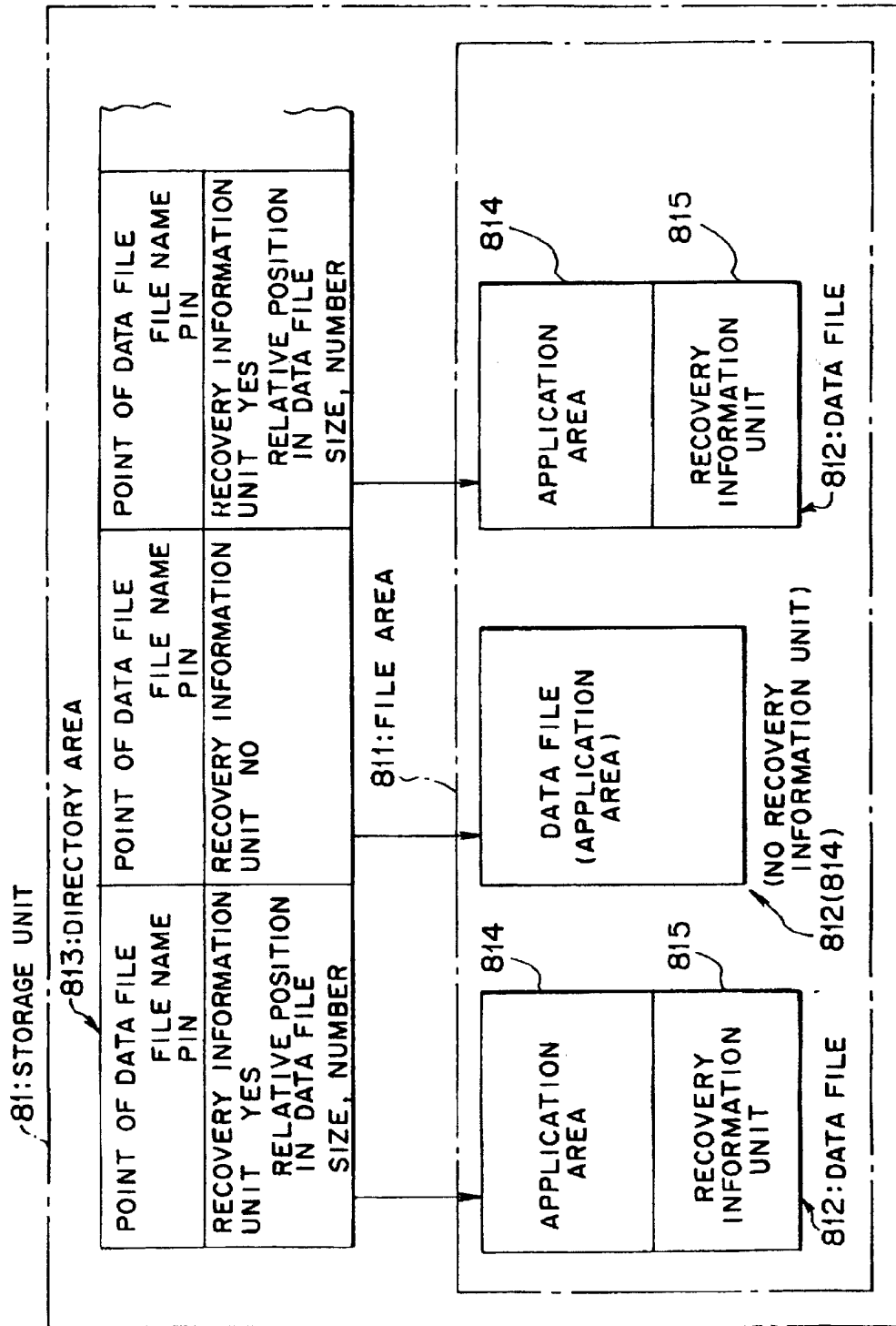


FIG. 10

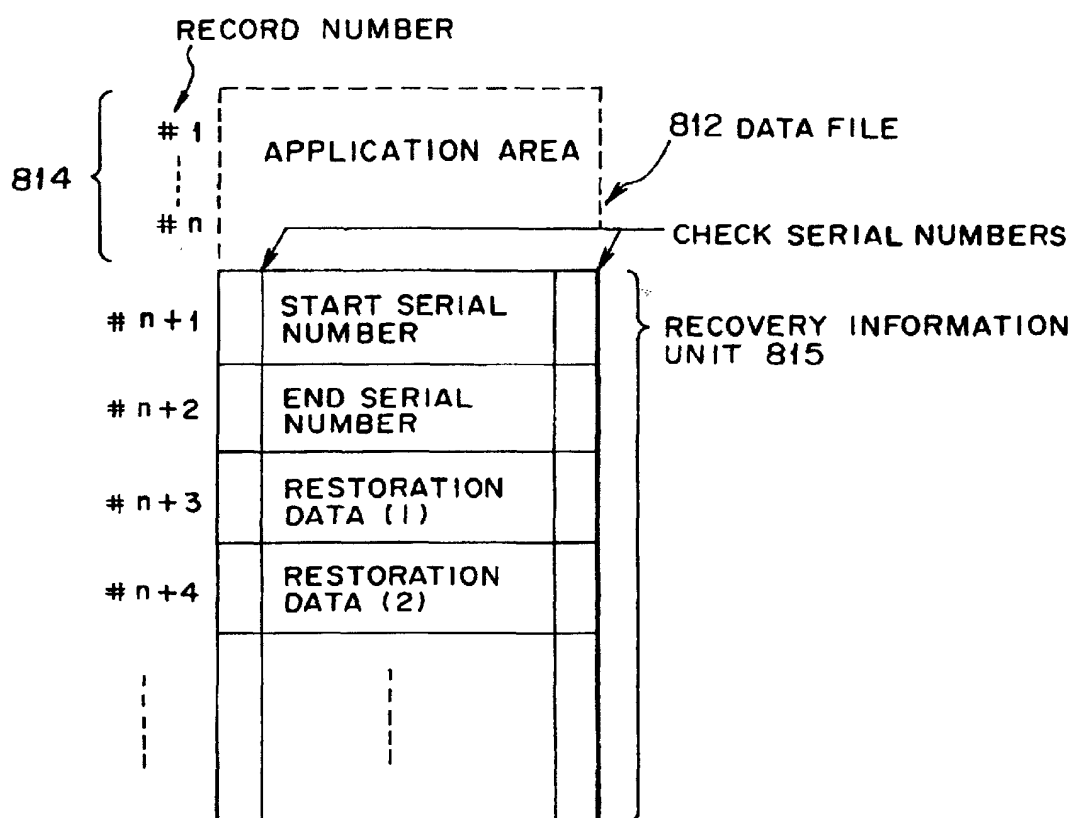


FIG. 11

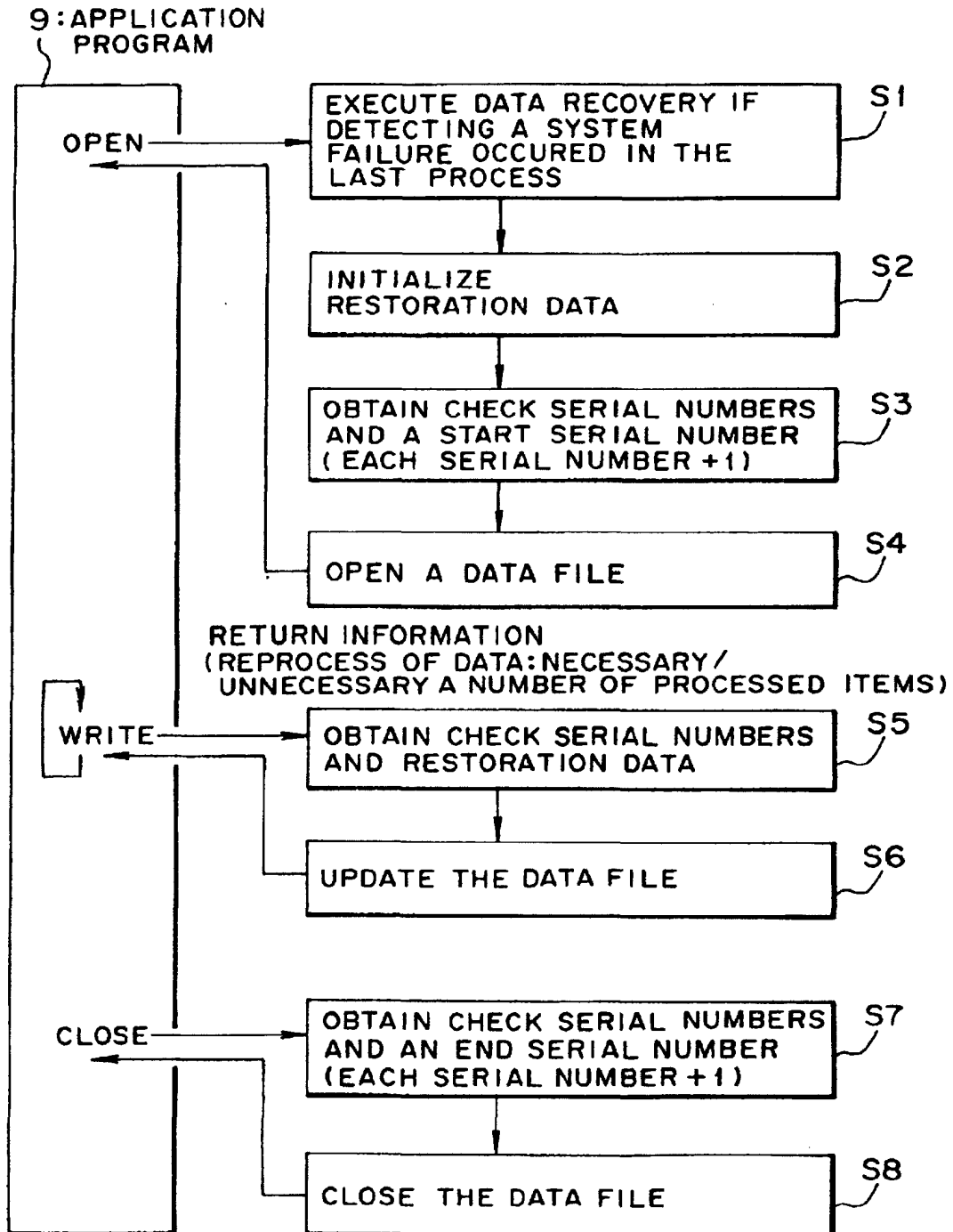


FIG. 12

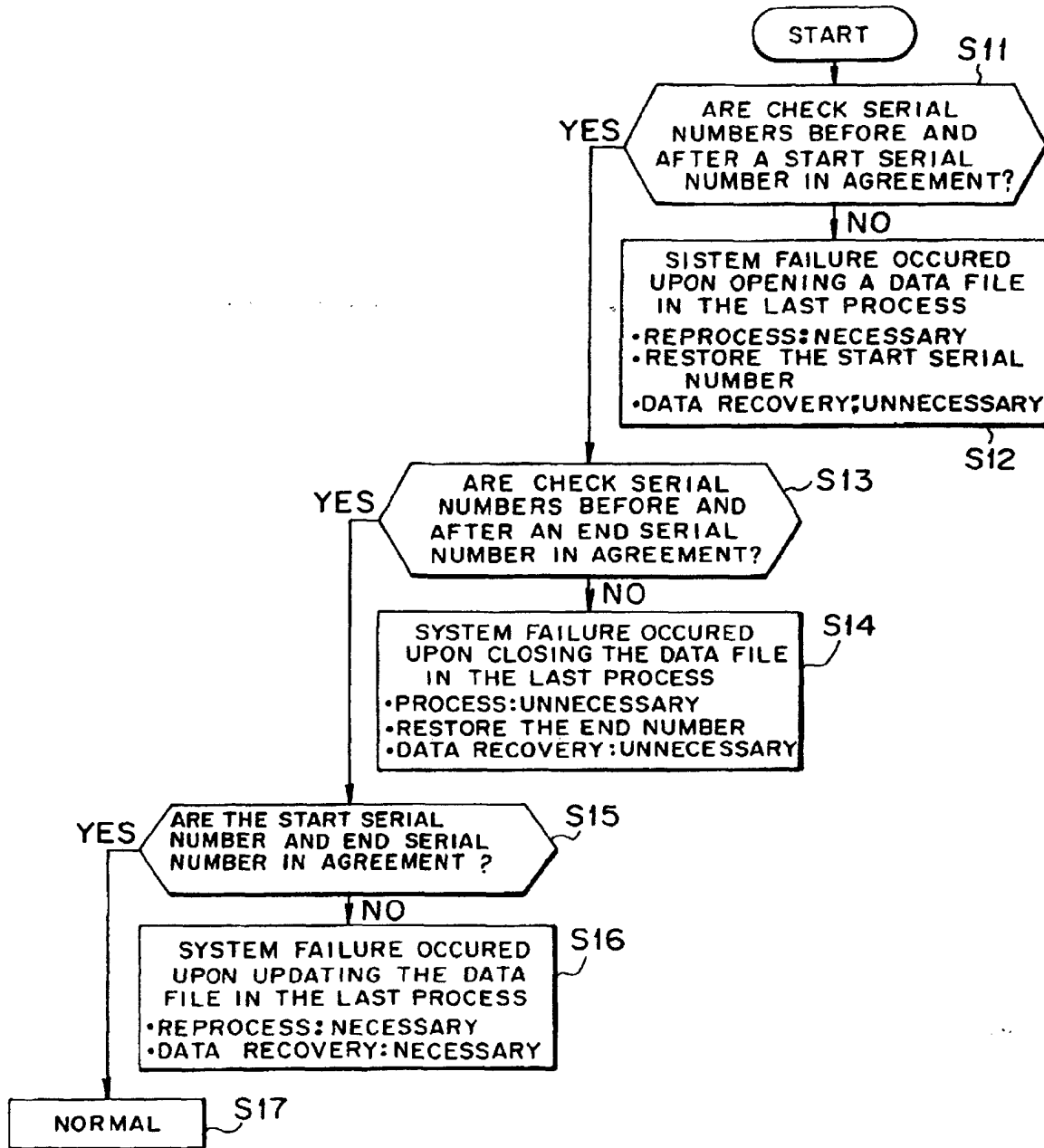


FIG. 13A

815

(IMMEDIATELY AFTER THE ISSUE)

START SERIAL NUMBER	1	00000000	1
END SERIAL NUMBER	1	00000000	1
RESTORATION DATA	1	00000000	1
	1	00000000	1
	1	00000000	1
CHECK SERIAL NUMBERS	1	00000000	1

FIG. 13B

815

(FIRST TIME)

2	00000001	2
2	00000001	2
2	#10,3030	2
2	#08,F1F1	2
2	#11,1010	2
1	00000000	1

↑ (APPLICATION)

9

OPEN
WRITE #10,--
WRITE #08,--
WRITE #11,--
CLOSE

FIG. 13C

815

(SECOND TIME)

3	00000002	3
3	00000002	3
3	#02 4040	3
1	00000000	1
1	00000000	1
1	00000000	1

↑ (APPLICATION)

9

OPEN
WRITE #02,--
WRITE #02,--
CLOSE

FIG.14

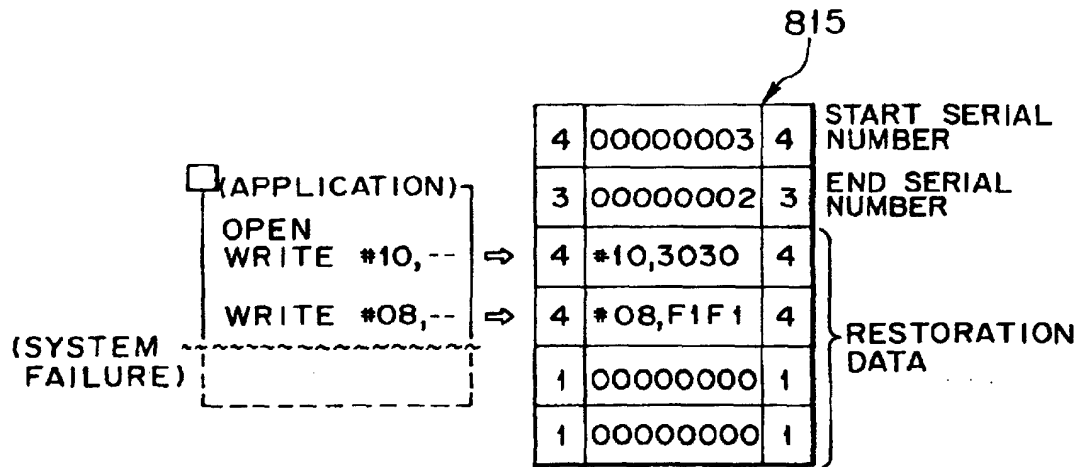


FIG.15

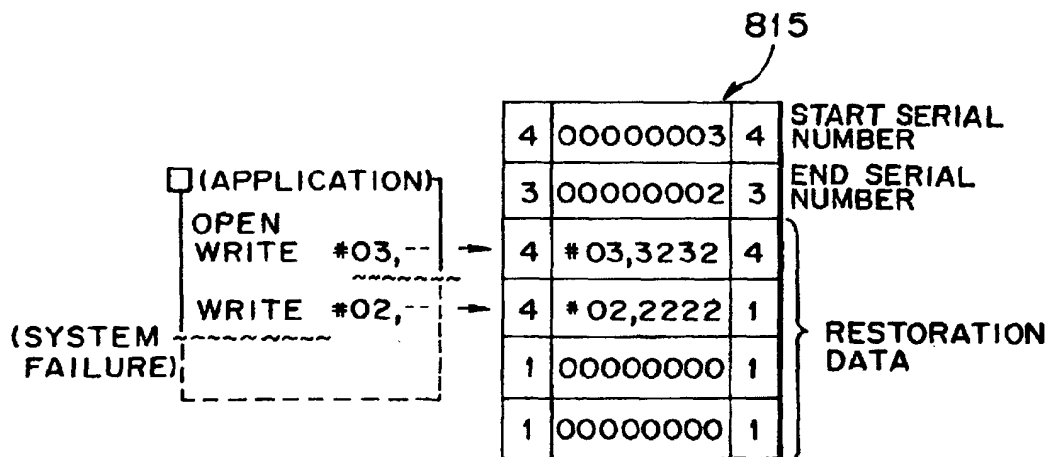


FIG.16A

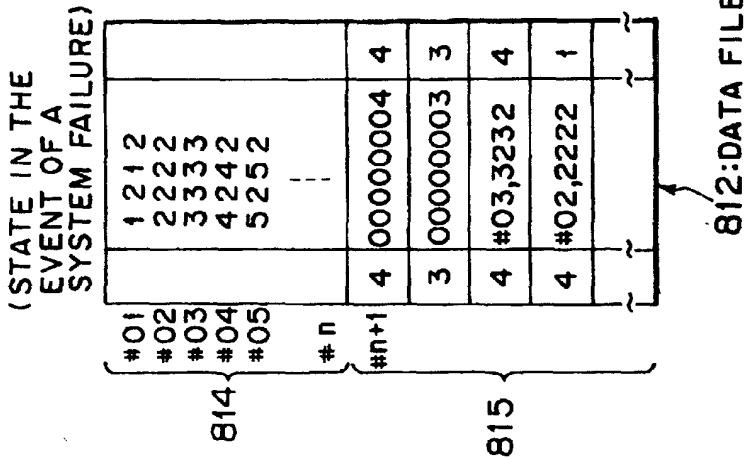


FIG.16B

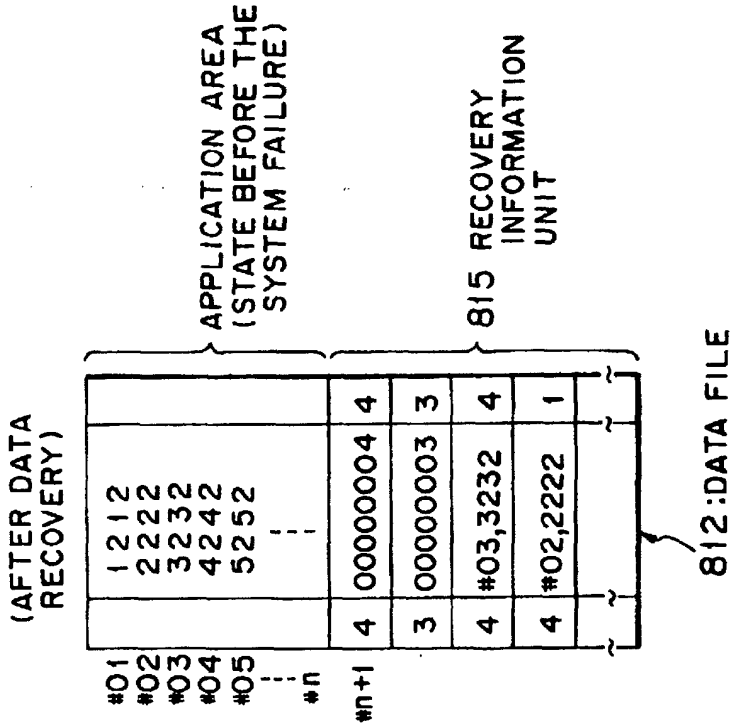


FIG. 17

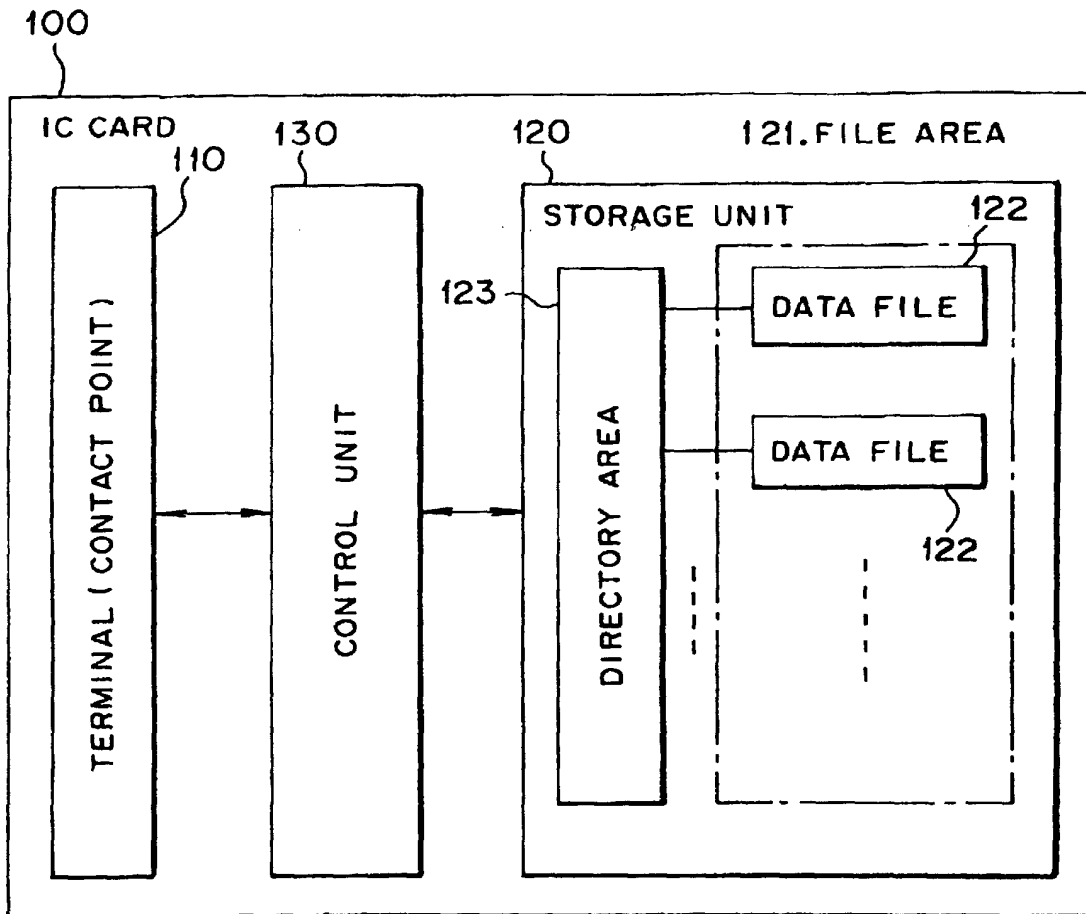


FIG. 18

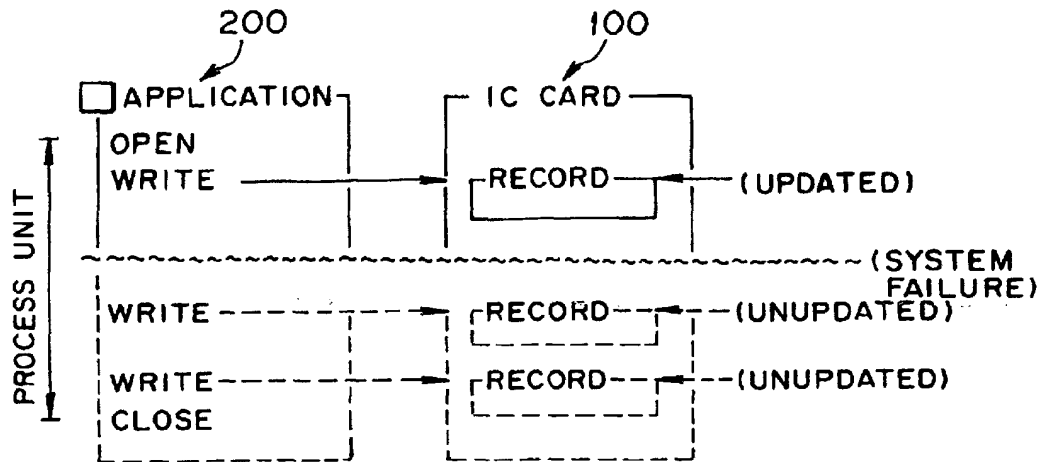


FIG. 19

